2019 | العدد 63



دراسات تنموية

مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي

د. علم الدين بانقا

سلسلة دراسات تنموية :

سلسلة تنموية تهدف إلى المساهمة في نشر الوعي بأهم قضايا التنمية عموماً، وتلك المتعلقة بالدول العربية خصوصاً، وذلك بتوفيرها لنصوص المحاضرات، وملخص المناقشات، التي تقدم في لقاءات علمية دورية وغير دورية يقوم بتنظيمها المعهد. ونظراً لحرص المعهد على توسيع قاعدة المستفيدين يقوم بتوزيع إصدارات السلسلة على أكبر عدد ممكن من المؤسسات والأفراد والمهتمين بقضايا التنمية الاقتصادية والاجتماعية، آملين أن تساهم هذه الإصدارات في دعم الوعي بالقضايا الاقتصادية والاجتماعية ونشر الآراء المختلفة للتعامل مع تلك القضايا في الدول العربية.

سلسلة دراسات تنموية
المعهد العربي للتخطيط بالكويت

مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي

إعداد

د. علم الدين بانقا

العدد (63)　　　　2019

المحتويات

تقديم

أدى ظهور التقنيات الجديدة في نظم المعلومات والتكنولوجيا الرقمية مثل انترنت الأشياء (Internet of Things) والحواجز المتسلسلة Block Chain وخدمات الحوسبة السحابية (Cloud services) الى ترابط غير مسبوق بين بلدان العالم والشركات والأفراد مما زاد من مخاطر الهجمات الإلكترونية الخبيثة. وازدادت في الآونة الأخيرة كثافة وخطورة هذه الهجمات مما جعل بعض المنظمات الدولية مثل صندوق النقد الدولي (IMF) والمنتدى الاقتصادي العالمي (WFE) تضع المخاطر الالكترونية في صدارة المخاطر النظامية (Systemic risk) التي تواجه النظام الاقتصادي العالمي وتدعو لبناء المنعة ضدها بسبب عِظَم آثارها الاقتصادية. وحاولت هذه الدراسة تسليط الضوء على أهمية هذه المخاطر وآثارها الاقتصادية وكيفية إدارتها، وأعطت نماذج دولية لحوادث الإصابة بها. ثم حلّلت وقيّمت أوضاع دول مجلس التعاون الخليجي كنموذج أو دراسة حالة. وهدفت من ذلك الى زيادة الاهتمام بالاستثمار في الأمن الإلكتروني واستدراك الثغرات في التخطيط الاقتصادي لمجابهة هذه المخاطر. وتأتي قطاعات الخدمات المالية والنفط في قائمة القطاعات المستهدفة عالمياً بالهجمات السيبرانية. وتتصدر دول مجلس التعاون الخليجي دول العالم الأخرى في بعض أنواع الهجمات السيبرانية على الأنشطة الاقتصادية مثل معدلات البرمجيات الخبيثة بالبريد الالكتروني ونسب البريد الالكتروني المؤذي (Spam). كما تفوق الخسائر الناجمة عن الهجمات الالكترونية في دول المجلس المتوسط العالمي ولا يمكن استرداد معظم الخسائر المالية الناجمة عنها.

وعلى الرغم من تحسن أداء دول المجلس في مجال مواجهة الهجمات الالكترونية، إلا أن الدليل العالمي للأمن السيبراني الذي تصدره الأمم المتحدة يشير إلى وجود العديد من الثغرات القانونية والفنية والتنظيمية والتدريبية والتعاونية التي يجب سدها من خلال تحسين الأداء والإكمال والمراجعة للوضع الراهن في هذه الجوانب. ولا تكفي زيادة الإنفاق بمفردها في مواجهة التهديدات وتحقيق الأمن السيبراني في دول المجلس، بل لابد من تحسين الوعي والحوكمة والعمليات (أو المعالجات) لأن هذه المنطقة هي إحدى أكثر مناطق العالم تقدماً في سرعة تبني واعتماد التكنولوجيا الحديثة.

المعهد العربي للتخطيط

أولاً: المقدمة

مع تنامي ثورة التكنولوجيا والمعلومات، أصبحت مخاطر الاقتصاد الشبكي من القضايا الجوهرية في الاستقرار الاقتصادي وتحقيق النمو المستدام. وبرزت مخاطر الهجمات الالكترونية كواحدة من أهم المخاطر النظامية (Systemic risk) التي تواجه الأنظمة الاقتصادية والمالية بسبب ازدياد التقارب التكنولوجي العالمي الذي أدى الى تبديد الفواصل المادية والرقمية بين دول العالم. وأشار المنتدى الاقتصادي العالمي ((World Economic Forum (WEF)) في تقريره عن المخاطر الدولية الى ارتفاع المخاوف من المخاطر التكنولوجية خصوصاً الهجمات السيبرانية وتزوير البيانات وظهرت هذه المخاطر في قائمة أعلى خمسة مخاطر دولية محتملة الحدوث في عام 2018. وبالمثل، تصدّرت التهديديات الالكترونية (السيبرانية) القائمة العالمية في المخاطر التي تواجه النظام المالي العالمي في العام 2018 وما بعده، وفقاً لاستطلاع الرأي الذي قامت به عدد من الجهات الدولية الأخرى مثل بنك إنجلترا ومؤسسة DTCC الأمريكية في عام 2017. وازدادت في الآونة الأخيرة كثافة وخطورة الهجمات السيبرانية الخبيثة سواء من جانب الانتشار أو في مقدرتها على التدمير وإلحاق الضرر بالمؤسسات الاقتصادية. وتضاعفت عدد الاختراقات السيبرانية التي تم تسجيلها من قبل قطاع الأعمال العالمي خلال الخمسة سنوات الماضية من 68 اختراق لكل منشأة في عام 2012 إلى 130 اختراق في عام 2017.

وعادت من جديد أسواق البرمجيات الخبيثة (Malware) بعد أن تم التضييق عليها بقوة القانون. وأُطلقت حوالي 357 مليون صنف من مختلف أصناف البرمجيات الضارة في عام 2016، وانخفض سعر البرمجيات الخبيثة التي تستخدم في سرقة بيانات الحسابات المصرفية (Banking Trojan) إلى حوالي 500 دولار للبرنامج الواحد. كما تضاعفت أعداد الضحايا المستهدفين من قبل مجرمي الانترنت (Cyber Criminals) بفضل ارتفاع استخدام خدمات الحوسبة السحابية (Cloud Services) وتوقع اتساع نطاق انترنت الأشياء (The Internet of Things) من حوالي 8.4 مليار جهاز مستخدم في عام 2017 إلى حوالي 20.4 مليار جهاز بحلول عام 2020، حتى أن الهجمات الالكترونية (أو السيبرانية) التي كانت تعتبر ضخمة في السابق قد أصبحت اليوم تبدو عادية جداً (WEF، 2018).

وكشف قطاع الشركات العالمية في عام 2016 عن حدوث أكثر من 4 مليار اختراق لسجلات البيانات وهي تعادل أكثر من ضعفي مجموع الاختراقات في العامين السابقين. كما ارتفعت عالمياً، نسبة الحرمان من خدمات الانترنت الموزعة Distributed Denial of Services (DDOS) بنسبة 140 % في عام 2016 وحدها. وازداد إصرار المهاجمين على إصابة المستهدف فارتفعت عدد الهجمات على نفس المستهدف إلى 32 مرة خلال ثلاثة أشهر في عام 2017. وارتفعت التكلفة المالية للهجمات الالكترونية (Cyber Attacks) حيث قدّرت احدى الدراسات العالمية التي أُجريت في عام 2017 على 254 شركة في سبعة دول عالمية أن متوسط التكلفة السنوية للتصدي لهذه الهجمات في الشركة الواحدة قد بلغ 11.7 مليون يورو، بنسبة زيادة سنوية قدرها 27.4 %. ومن المتوقع أن ترتفع تكلفة الجرائم الالكترونية (Cyber Crimes) على قطاع الأعمال في غضون الخمسة سنوات القادمة إلى حوالي 8 تريليون دولار (Global Risk Report 2018). وقد قدّر مجلس المستشارين الاقتصاديين الأمريكي حجم الخسائر الناجمة عن الأنشطة السيبرانية الخبيثة في امريكا في عام 2016 بمبلغ يتراوح بين 57-109 مليار دولار (Council of Economic Advisors (CEA), 2018).

وقد مثّلت الفدية المالية التي تدفع لمجرمي الانترنت أكبر أنواع التكاليف المالية للهجمات الالكترونية على الشركات في عام 2017. وترتبط هذه الفدية بتزايد الهجمات الالكترونية الضارة على المستهدفين وذلك من خلال عزلهم عن قواعد بياناتهم ثم المطالبة بالفدية في مقابل إعادة الوصول للبيانات. كما مثّلت الهجمات الخبيثة المطالبة بالفدية نسبة 64 % من جملة الهجمات الضارة على البريد الالكتروني (Emails) المرسل بين شهري يوليو وسبتمبر في عام 2017 ليتأثر بها ضعف عدد الشركات المتأثرة في عام 2016.

وتتمثل المشكلة الاقتصادية للهجمات الالكترونية الخبيثة في عدم قصورها على المؤسسة المستهدفة وحدها وانتشار آثارها الخارجية السلبية (Negative Externalities) الى القطاعات الأخرى، خصوصاً في المؤسسات التي تعمل في مجال البنية التحتية الحيوية والتي قد تنتشر عبرها الآثار السلبية للهجمات إلى الأنشطة الاقتصادية الأخرى فتتعطل تلك الأنشطة، مما يفاقم الخسارة الناجمة عن هذه الهجمات. ويعتبر الأمن الالكتروني (أو السيبراني) سلعة عامة (Public Good) ويؤدي التراخي فيها على مستوى الدولة والمؤسسات الى إلحاق آثار خارجية

سلبية بالمؤسسات الأخرى والأفراد بل وبالدول الأخرى بسبب تشابك الأنظمة الالكترونية واعتمادها على بعضها البعض. وفي العادة، تنتشر أضرار الهجمات السيبرانية الخبيثة من المؤسسة المستهدفة إلى مؤسسات أخرى مرتبطة بها اقتصادياً مثل الموردين مما يتسبب في تفاقم الخسائر بالنسبة لاقتصاد الدولة الكلي. ويؤدي عدم أخذ صانعي القرار في المؤسسات للآثار الخارجية السلبية للهجمات في الاعتبار إلى ضعف الاستثمار في الأمن السيبراني ويزيد من المخاطر الكلية على المؤسسات.

وتهدف هذه الدراسة الى تسليط الضوء على أهمية المخاطر والهجمات الالكترونية والآثار الاقتصادية الكبيرة الناجمة عنها في دول مجلس التعاون الخليجي خصوصاً وأن هذه الدول تسعى الى التحول الى اقتصادات قائمة على المعرفة مما يتطلب ضرورة مواجهة تهديدات الاقتصاد الشبكي ومراجعة الخطط الاستراتيجية للأمن الالكتروني وسد الثغرات القائمة فيها.

وتتبع أهمية الدراسة من ازدياد كثافة الهجمات والتهديدات الالكترونية في دول مجلس التعاون الخليجي وارتفاع تكاليفها المالية والاقتصادية في المنطقة مقارنة مع المناطق العالمية الأخرى. بالإضافة الى قلة الدراسات الاقتصادية التي تحلّل وتقيّم المخاطر الالكترونية في الدول العربية وتحاول الوصول الى نتائج وتوصيات تساعد صانعي القرار في سد الثغرات في هذا المجال وتقديم حلول عملية من خلال تقييم تجارب الدول الأخرى والمؤسسات الرائدة في هذا المجال.

تقوم هذه الدراسة بتحليل واقع وتحديات الأمن السيبراني بدول مجلس التعاون الخليجي ومقارنة أوضاعها مع الدول الأخرى والتعرف على خصوصية المخاطر الالكترونية التي تواجهها من جانب نوعية وكثافة الهجمات والقطاعات المستهدفة ومستوى نجاحها والاضرار الناجمة عنها، فضلاً عن اعطاء نماذج لها وكيفية التعامل معها. وتسعى الدراسة الى بيان طرق ونماذج تعزيز المنعة لمواجهة المخاطر الالكترونية على مستوى الدولة والمؤسسة في الدولة.

وقد واجهت هذه الدراسة مشكلة شح البيانات عن الهجمات الالكترونية بسبب عدم افصاح المؤسسات المستهدفة عنها ومشاركتها مع المؤسسات الأخرى سواءً على المستوى الاقليمي أو الدولي لما للإفصاح من الآثار الاقتصادية والمالية الكبيرة على سمعتها ونزاهتها وقيمتها السوقية. كما أن المؤسسات في المنطقة غالباً ما تجد صعوبة في تحديد وقت وقوع الهجوم ونوعه ولا تكتشفه إلا عندما يتم الإبلاغ عنها من أطراف ثالثة أو من عملاء أو عند ورود طلبات من الجهات المهاجمة للحصول

على أموال الفدية في حالات الهجمات المالية. ولهذه الأسباب يعتمد الباحثون في مخاطر الهجمات السيبرانية عموماً على البيانات المتاحة من طرف ثالث مثل تقارير الشركات العالمية للأمن السيبراني والجهات الحكومية والخاصة ذات الصلة بهذا المجال.

وتحتوي هذه الدراسة على مقدمة وثمانية محاور وهي: مفاهيم ومصطلحات أساسية، أمثلة ونماذج عالمية للهجمات الالكترونية، إدارة المخاطر الالكترونية ونماذج التعامل مع هذه الهجمات، واقع وأهمية المخاطر الالكترونية على المستوى العالمي، واقع وأهمية المخاطر الالكترونية في دول مجلس التعاون الخليجي، أمثلة ونماذج من دول المجلس للهجمات الالكترونية، تقييم الآثار الاقتصادية للهجمات الالكترونية على دول مجلس التعاون الخليجي، الخاتمة والتوصيات.

ثانياً: مصطلحات ومفاهيم أساسية

سنوضح في البدء بعض المصطلحات الأساسية في الأمن الالكتروني ثم نُعرّف المقصود من الأنشطة السيبرانية الخبيثة والجهات الفاعلة في مجال التهديد الإلكتروني والتي تنقسم الى ست مجموعات عريضة وهي: الدول القومية، الشركات المنافسة، والقراصنة، الجماعات الإجرامية المنظمة، الانتهازيون، والمطلعين على الشركة (Company insiders). وفيما يلي بعض المصطلحات في الأمن الالكتروني التي سوف نستخدمها في الدراسة.

- سايبر (الكتروني) Cyber: تعني كلمة سايبر ترابط البنيات التحتية لشبكات تكنولوجيا المعلومات، وتضم أدوات أو وسائل التكنولوجيا مثل الانترنت، شبكات الاتصالات، أنظمة الحاسوب، وما تتضمّنه من معالِجات (Processors) ومجمِعات (Collectors) في الصناعات المهمة ذات الصلة.
- الأمن السيبراني (أو الالكتروني) Cyber Security: تعني التحليل، الإنذار، تشارك المعلومات، تقليل التعرض للمخاطر الالكترونية، تخفيف المخاطر، وجهود الاستفادة من النظام الشبكي للمعلومات.
- المخاطر السيبرانية (أو الالكترونية) Cyber Risks: وهي عبارة عن مزيج من احتمالية وقوع الحادثة داخل شبكات نظم المعلومات وآثار هذا الحدث على أصول المؤسسة

وسمعتها. وتعتبر المخاطر الالكترونية مشكلة تجارية ذات أبعاد تقنية، ويؤثر هذا النوع من المخاطر على كل مجالات المؤسسة ويتأثر بها من جانب احتواء المخاطر أو تضخيمها.

- التهديدات السيبرانية (أو الالكترونية): هي عبارة عن أحداث الكترونية محتملة ينتج عنها نتائج غير مرغوب فيها تسبب ضرراً للأنظمة أو للمؤسسة، وقد تنشأ هذه التهديدات داخلياً أو خارجياً ومن الأفراد أو المؤسسات.
- القابلية للإصابة بالأضرار السيبرانية (أو الالكترونية) Cyber Vulnerabilities: وهي عبارة عن درجة الحساسية ومدى كفاية الدفاعات في حماية أصل واحد أو مجموعة من أصول المؤسسة وإمكانات مواجهة التهديدات الالكترونية.
- القيم الأساسية التي في الخطر Primary Values at Risk: هي عبارة عن أصول المؤسسة الملموسة وسمعتها المعرضة للإصابة بالتهديدات السيبرانية. وعند الأخذ في الاعتبار التبعيات الكبيرة للتهديدات، فإن العواقب على أصول المؤسسة يمكن أن تؤدي الى حوادث كبيرة ومتتالية تتجاوز سيطرة المؤسسة.
- إدارة المخاطر الالكترونية Cyber Risk Management: تسعى إدارة المخاطر الالكترونية إلى التأثير على السلوك البشري والأعراف والضوابط الفنية والتفاعلات بين الآلة والآلة وتهدف إلى تنسيق الأنشطة والمعالجات لمنع حدوث اي عواقب ونتائج غير مرغوب فيها.
- تقييم المخاطر Risk Assessment: هي العملية التي تقوم بها المؤسسة لتحليل وتقييم وفهم مجموعة من المخاطر التي تواجهها واحتمالية وقوعها وشدتها وذلك بهدف التمكُّن من خفضها إلى مستوى مقبول.
- استراتيجية تحويل المخاطر Risk Transfer Strategy: وهي تمثّل احدى طرق التعامل مع المخاطر التي تواجه المؤسسة ومن أمثلتها: التأمين، التعويض، وحلول نقل المخاطر الهيكلية Structured risk-transfer solutions.
- بناء المنعة السيبرانية (أو الالكترونية) Cyber Resilience: وهي احدى أجزاء إدارة المخاطر الالكترونية. ويمكن تعريفها بأنها مقدرة الأنظمة والمؤسسات على تحمل ومواجهة الأحداث السيبرانية ويمكن قياسها من خلال مزيج من متوسط الوقت إلى الفشل

ومتوسط الوقت إلى التعافي Meantime to failure and meantime to recovery.

- المخاطر النظامية في النظام المالي: هي المخاطر الكامنة في السوق بأكمله أو في قطاع منه. ويؤثر هذا النوع من المخاطر على السوق ككل، وليس فقط على سهم أو صناعة معينة. وهذا النوع من المخاطر لا يمكن التنبؤ به ويستحيل تجنبه تمامًا. وينتج عن هذا النوع من المخاطر عادة تغيّر في المتغيرات الاقتصادية الكلية في الدولة (WEF، 2012).

الأنشطة الالكترونية الخبيثة والجهات الفاعلة في ممارسة التهديد الإلكتروني

يُعرّف القانون الأمريكي النشاط الإلكتروني (السيبراني) الخبيث بأنه نشاط، غير مرخص به من قِبل القانون الأمريكي، والذي يسعى إلى الحصول على تنازلات من جهة ما أو يتسبب في اضعاف السرية أو النزاهة أو تعطيل توافر نظم الحواسيب أو المعلومات أو الاتصالات أو الشبكات والبنية التحتية المادية أو الافتراضية التي تتحكم فيها أجهزة الكمبيوتر أو أنظمة المعلومات، أو المعلومات الموجودة فيها. وتتخذ الأنشطة الالكترونية الخبيثة الموجهة للشركات أشكالاً متعددة، كلها تُضعِف واحدة أو أكثر مما يعرف بـ "ثلاثية (CIA)" والتي تعني: السرية (Confidentiality)، النزاهة (Integrity) والتوافر (Availability). فعلى سبيل المثال، يُعرف هجوم رفض الخدمة الموزعة (DDoS) بأنه هجوم خبيث يجعل الخدمة عبر الإنترنت غير متوفرة من خلال إرباكها والتغطية عليها بحركة كثيفة من مصادر متعددة، فيندرج هذا الهجوم تحت فئة "التوافر" من الثلاثية السابقة لأنه يعترض تقديم الشركة لخدماتها على شبكة الإنترنت. وبالمثل فإن سرقة الأموال من حساب عميل مصرفي من خلال الطرق السيبرانية يؤدي الى انتهاك نزاهة بيانات معاملات المصرف فتندرج هذه الجريمة تحت فئة "النزاهة". كما ان سرقة البيانات الشخصية التعريفية (PII) الخاصة بزبائن الشركة أو الموظفين بالطرق السيبرانية تُضعِف خصوصية معلومات الشركة فتندرج هذه الجريمة تحت فئة "السرية أو الخصوصية" (CEA USA, 2018).

وتشمل حوادث الأمن السيبراني الحالات التالية، على سبيل المثال لا الحصر (1) المحاولات الناجحة والفاشلة للوصول غير المصرح به إلى النظام الشبكي للمؤسسة أو بياناته؛ (2) هجمات الحرمان من الخدمة الموزعة DDoS؛ و (3) إحداث تغييرات غير مصرح بها على أجهزة ومعدات النظام أو البرامج الثابتة أو البرمجيات في المؤسسة.

وتنقسم الجهات الفاعلة في مجال التهديد الإلكتروني إلى ست مجموعات عريضة، يقود كل منها مجموعة متميزة من الأهداف والدوافع وهي:

(1) الدول القومية: وهذه المجموعات تكون ممولة بشكل جيد وغالباً ما تنخرط في هجمات متطورة وموجهة. وعادة ما تكون الدول القومية مدفوعة بجداول أعمال سياسية أو اقتصادية أو تقنية أو عسكرية. وكثيرا ما تشارك الدول القومية في التجسس الصناعي. وإذا كانت لديهم احتياجات تمويلية، فقد يقومون بهجمات فدية وسرقات إلكترونية للأموال. وغالباً ما تستهدف الدول القومية معلومات تحديد الهوية الشخصية (PII) للتجسس على أفراد معينين. كما قد تنخرط هذه الدول في تدمير واحدة أو أكثر من شركات الدولة المستهدفة، ويحتمل أن يكون ذلك بمثابة انتقام ضد العقوبات أو غيرها من الإجراءات التي يتخذها المجتمع الدولي.

(2) الشركات المنافسة: تسعى هذه الشركات للحصول غير المشروع على البيانات الخاصة بالملكية الفكرية (PI) لشركة منافسة في نفس الدولة أو في دول أخرى، بما في ذلك المعلومات المالية والاستراتيجية والقوى العاملة فيها؛ وكثيراً ما تدعم هذا النوع من الهجمات الدول القومية لتعزيز منافسة شركاتها عالمياً.

(3) القراصنة: يمارس القرصنة عموماً أفراد أو مجموعات خاصة في جميع أنحاء العالم لديهم أجندة سياسية ويسعون لتنفيذ هجمات عالية المستوى. وتساعد هجمات القرصنة الالكترونية على نشر الدعايات أو إلحاق الضرر بمنظمات المعارضة لأسباب أيديولوجية.

(4) الجماعات الإجرامية المنظمة: هذه جماعات إجرامية تمارس هجمات استهدافية بدافع الربح. ويجمعون العوائد عن طريق بيع البيانات الشخصية (PII) المسروقة على شبكة الإنترنت ومن خلال تحصيل مدفوعات الفدية من القطاعين العام والخاص ومن خلال الهجمات التخريبية.

(5) الانتهازيون: هؤلاء عادة قراصنة هواة مدفوعين برغبة في الشهرة. وفي العادة يهاجم الانتهازيون المنظمات التي تستخدم الرموز (codes) والأساليب المتاحة على نطاق واسع، وبالتالي عادة ما تمثّل هذه المجموعات أقل أشكال الجماعات المهاجمة تقدماً.

(6) المطلعين على الشركة (Company insiders): عادة ما يكون هؤلاء هم الموظفون الساخطون أو الموظفون السابقون الذين يبحثون عن الانتقام أو الربح المالي. وتزداد خطورة المطلعين على بواطن الأمور في الشركة بشكل خاص عندما يعملون جنباً إلى جنب مع جهات خارج الدولة، مما يسمح لهذه الجهات الخارجية بسهولة تجاوز حتى أقوى الدفاعات السيبرانية (CEA USA, 2018).

ثالثاً: أمثلة ونماذج عالمية لمخاطر الهجمات الالكترونية

من أشهر الأمثلة لهذه الهجمات الإلكترونية في عام 2017 الهجمة المسماة Wannacry، وهي برمجية خبيثة تطالب الضحية بالفدية المالية وقد أثرت على 300.000 جهاز حاسوب في 150 دولة في العالم، وهجمات Petra و Not Petra، والتي تسببت في الحاق خسائر فادحة في بعض الشركات العالمية. فعلى سبيل المثال، أعلنت شركات FedEx , Merck، Maersk خسائر تقدر بحوالي 300 مليون دولار بسبب هذه الهجمات. بالإضافة إلى التكاليف المالية، فقد تسبب هجمات Wannacry في تعطيل بيانات أساسية استراتيجية على مستوى العالم. شمل هذا التعطيل وزارات حكومية وسكك حديدية وبنوك ومقدمي خدمات اتصالات وشركات مقدمة لخدمات الطاقة، وصانعي سيارات ومستشفيات. مما جعل ظهور هذه الهجمات يهدد بانهيار الأنظمة التي تحفظ قيام المجتمع بمهامه الأساسية في كثير من البلدان. ويتعاظم الخطر من هذه الهجمات الضارة لأن العديد منها تتم برعاية دول عالمية في بعض الأحيان.

وقد أوضحت تجربة هجمات Wannacry أن البنيات التحتية للعديد من المؤسسات قد تكون ذات قابلية عالية للتعطيل بسبب هذه الهجمات، خصوصاً بعد حالة الاعتداء التي حدثت على قطاع الطاقة الأوكراني في عام 2015 والذي أدى إلى إغلاق مؤقت لأكثر من 30 محطة توليد طاقة فرعية وقطع إمداد الطاقة عن أكثر من 230 ألف شخص. وأعلنت وكالة سلامة الطيران

الأوروبية European Aviation Safety Agency أن أنظمة الطيران تتعرض إلى ما يعادل 1.000 هجوماً شهرياً في المتوسط. كما شهد عام (2017) ارتفاع عدد محاولات التصيّد الاحتيالي (Spear-Phishing) من خلال سرقة البيانات الشخصية أو تركيب برمجيات ضارة عن طريق استخدام البريد الالكتروني المحتال (email scam). وقد استهدفت بعض هذه الهجمات شركات تشغيل الطاقة النووية في أمريكا.

وعلى الرغم من فشل معظم الهجمات الالكترونية على الأنظمة الاستراتيجية الأساسية، الا أن نجاح بعض هذه الهجمات المنفردة وتزايد أعدادها يؤكّد ارتفاع مخاطر هذه الهجمات، هذا إذا أخذنا في الاعتبار ازدياد ترابط وتشابك النظام العالمي الاقتصادي والمالي مما قد يؤدي إلى إعاقة في بعض الأنظمة التي لا يمكن إلغاؤها والتغلب عليها (Global Risk Report 2018). وتوضح النماذج التالية بعض أصناف الهجمات الالكترونية التي حدثت في دول عالمية متعددة. ويُقصد من سرد هذه النماذج توضيح ضخامة حجم الاضرار التي تلحق بالمؤسسات والافراد جراء الهجمات الالكترونية الخبيثة وتعدد الأسباب التي تُستهدَف من أجلها هذه المؤسسات. وتتضمّن هذه النماذج الأصناف التالية من الهجمات:

(1) سرقة البيانات الخاصة لملايين الأشخاص من موقع واحد على الانترنت.

(2) تدمير الشركات المنافسة.

(3) سرقة البنوك المركزية والخاصة.

(4) انتشار الآثار الخارجية السالبة (Externalities and spillovers) للهجوم الخبيث.

(5) استغلال الثغرات والحلقات الضعيفة.

نماذج لمخاطر الهجمات الالكترونية

3.1 سرقة البيانات الخاصة لملايين الأشخاص

شركة Equifax الأمريكية هي ثالث أكبر وكالة ائتمانية في أمريكا بعد رصيفاتها Experian, Trans Union. تأسست في أطلنطا Atlanta في عام 1899 وتقوم

بجمع بيانات لأكثر من 800 مليون مستهلك و88 مليون مؤسسة تجارية حول العالم. أعلنت الشركة عن اختراق خطير للبيانات الشخصية التي تحتفظ بها في يوم 2017/9/7. وقد تمكّن مجرمو الانترنت من الوصول إلى البيانات الشخصية لأكثر من 140 مليون شخص تتضمن الأسماء والعناوين وأرقام الضمان الاجتماعي. وقد حدث الاختراق في شهر يوليو 2017، وقبل أن تعلن الشركة عن الاختراق في سبتمبر 2017، قامت ببيع عدد من الأسهم تعادل 2 مليون دولار. وبعد أن أعلنت الشركة عن الاختراق انخفضت أسعار أسهمها بنسبة 13.7 % في اليوم التالي للإعلان. ونتيجة لضخامة الحدث، قامت السلطات الأمنية باستجواب المدير التنفيذي للشركة بتهمة التداول من الداخل (Insider Trading) والتي استقال من منصبه بسببها. وفقدت أسهم الشركة 34.9 % من قيمتها كمحصلة الاختراق وكادت الشركة أن تنهار وتفاقمت شكوك المستثمرين حول مستقبل الشركة، مما حدّ من مقدرتها على الحصول على التمويل المستقبلي.

ويوضح هذا الحادث أن نجاح محاولة واحدة من الهجمات الكترونية قد تلحق الاضرار المالية والاجتماعية بملايين الأفراد والمؤسسات التجارية مما يجعل المخاطر الالكترونية تمثّل التحدي الأكبر في الاقتصاد الرقمي.

3.2 تدمير الشركات المنافسة

تمارس بعض الشركات العالمية المنافسة الجائرة في أسواق الدول الأخرى بهدف اقصاء وتدمير الشركات المنافسة لها وقد تدعم بعض هذه الممارسات الحكومات القومية بهدف تمكين شركاتها الوطنية من السيطرة على بعض الأسواق العالمية. وتستخدم الهجمات السيبرانية كوسيلة لتحقيق هذه الأهداف، وغالباً ما يتم ذلك عن طريق سرقة الملكية الفكرية للشركات المستهدفة. وتعتبر سرقة الملكية الفكرية (IP: Intellectual Property) هي الجريمة الأعلى تكلفة من بين الجرائم السيبرانية، وذلك بسبب عدم تمكن الشركة المخترقة من اكتشاف الاختراق لعدة سنوات مما يتيح للمجرمين استخدام ملكيتها الفكرية ويلحق الضرر بها. وتتأثر بهذا النوع من الاختراق بصورة أكبر الشركات التي ترتكز في أنشطتها على مجال ضيق من الملكية الفكرية. ونستعرض نموذج سرقة الملكية الفكرية والمعلومات الخاصة بشركة Solar World AG الألمانية بواسطة الشركات المنافسة الصينية.

تقوم شركة Solar World AG بصنع وتسويق منتجات حصاد الطاقة الشمسية، ولها فروع في عدة دول منها أمريكا. وقد تم اختراق الشركة بواسطة شركات منافسة صينية خلال الفترة من مايو الى سبتمبر في عام 2012. وأعلنت السلطات الفدرالية الأمريكية في مايو 2014، الملاحقة القضائية لخمسة أشخاص صينيين بتهمة التجسس، سرقة الأسرار التجارية، والاحتيال للقرصنة على 6 شركات أمريكية والتي تتضمن شركة Solar World AG فرع أمريكا، خلال فترة 8 سنوات. وقد تمت سرقة آلاف الإيميلات والملفات الخاصة بالمدراء التنفيذيين خلال 13 هجوم خبيث.

وتحتوي هذه المعلومات المسروقة على بيانات عن الوضع المالي لشركة Solar World AG، وعن إمكانياتها الإنتاجية، وتكاليف إنتاجها، وخطة عملها واستراتيجيتها. وتمكّن المنافسون الصينيون من خلال اختراق أنظمة Solar World AG من الحصول على معلومات تجعلهم في وضع تنافسي أفضل في الأسواق الامريكية. فعرفوا من خلال بيانات التدفقات النقدية للشركة، المدة الزمنية التي تستطيع أن تتحمّلها الشركة عند حدوث صدمة ما، وتمكنوا من استنساخ أساليب الإنتاج والتصنيع دون الحاجة لبذل المال والبحث العلمي في تطوير هذه الأساليب. كما مكّنت بيانات تكاليف الإنتاج الشركات الصينية المنافسة من تسعير منتجاتها بأسعار منخفضة تجعل أسعار الشركة المنافسة غير مقبولة للزبائن.

وتحصل الصينيون، من خلال هذا الاختراق السيبراني الخبيث على مزايا تنافسية، مكّنتهم من إلحاق الضرر البليغ بشركة Solar World AG بسبب فقدانها الميزة التنافسية في الأجل الطويل والعائد على الاستثمار وكانت نتيجة ذلك أن خسرت هذه الشركة 35% من قيمتها السوقية والتي تعادل خسارة 178 مليون يورو. وفي مايو 2017، تقدمت الشركة بطلبها لقانون تسوية الإفلاس وتم عرض فرع الشركة بأمريكا للبيع لمساعدة الشركة الأم على الوفاء بديونها المتعثرة.

ويوضح هذا النموذج مقدرة البرمجيات الخبيثة المهاجمة على تدمير الخصم وإلحاق الضرر الاقتصادي البليغ ومنح مزايا تنافسية سوقية غير مستحقة لشركات غير قادرة على الابتكار.

3.3 سرقة البنوك المركزية والتجارية

في مارس 2016، أعلن بنك بنغلاديش المركزي عن سرقة 81 مليون دولار من حسابه في بنك نيويورك الفيدرالي. فقد تمكّن بعض القراصنة من الوصول إلى أنظمة بنك بنغلاديش المركزي وأرسلوا منه رسائل عبر نظام السويفت SWIFT: Society for Worldwide Interbank-Financial Telecommunications إلى بنك نيويورك الفيدرالي يطلبون فيها تحويل ما يقارب مليار دولار من احتياطات بنك بنغلاديش النقدية وإيداع المبالغ في حسابات في الفلبين وسريلانكا. ومن بين 35 طلب أُرسلت، تمت الاستجابة لأربعة طلبات فقط والتي تم من خلالها تحويل مبلغ 81 مليون دولار من حساب بنك بنغلاديش لحسابات في الفلبين لتُستخدم وتُبيّض فيها تلك الأموال عبر صناعة القمار.

وبعد الإفصاح عن سرقة بنك بنغلاديش المركزي، ظهرت مجموعة من السرقات لم يتم الإفصاح عنها مسبقاً. فقد تمكّن القراصنة في عام 2015 من سرقة شهادات اعتمادات من نظام السويفت ونجحوا في تحويل 12 مليون دولار من حسابات بنك Banco Del Austro الأكوادوري في بنك Wells Fargo الأمريكي. وبالمثل، تمت سرقة أكثر من 60 مليون دولار من بنك الشرق الأقصى الدولي التايواني Taiwanese for Eastern International Bank.

وقد أوضحت شركات الأمن السيبراني أن هذه الحوادث مرتبطة ببعضها، وعزت هذه السرقات إلى هجمات سيبرانية من مجموعة لازورس (Lazurus Group) وهي مجموعة إجرامية تعمل منذ عام 2009 وتدعمها كوريا الشمالية. وقد قامت هذه المجموعة بعدة هجمات على القطاع المالي وعلى أهداف أخرى في الأراضي الأمريكية مثل الهجوم على شركة سوني في أمريكا في حادثة Sony Pictures والتي حدثت في عام 2014 (CEA USA، 2018).

3.4 الآثار الخارجية السلبية للهجوم الخبيث (Externalities) وانتشارها للقطاعات الأخرى (Spillovers)

انتشرت، على سبيل المثال، الآثار السلبية للهجوم الخبيث على وكالة Equifax الائتمانية للشركات المثيلة في نفس القطاع كما تأثرت الشركات المرتبطة بها عبر الموردين مثل الشركات المصدرة

للبطاقات الائتمانية نذكر منها شركة Scherbina and Schlusche. فقد تأثرت أكبر وكالتين للائتمان في أمريكا وهما وكالة Trans Union ووكالة Experian سلباً بنجاح الهجوم السيبراني الخبيث على شركة Equifax، لأنه أثار مخاوف العملاء من حدوث اختراق مماثل لهذه الشركات أيضاً، مما أدى إلى تجميد الائتمان في الشركات الثلاث، كما أعلنت الجهات الرقابية بفرض إجراءات رقابية أكثر صرامة على الشركات الثلاثة لمنع الاختراقات المماثلة في المستقبل. وقد انخفضت قيمة أسهم هذه الشركات بنسبة 18% نتيجة للهجوم على شركة Equifax. كما انخفضت أسهم شركات الموردين والمستخدمين المرتبطة بها بنسبة 9% لذلك أيضاً.

3.5 استغلال الثغرات والحلقات الضعيفة

تم اختراق شركة Home Depot الأمريكية العاملة في مجال الأجهزة والمعدات المنزلية في إبريل 2014، مما نتج عنه تسريب بيانات بطاقات دفع الكتروني تصل إلى حوالي 56 مليون بطاقة، بالإضافة إلى تسريب 53 مليون بريد الكتروني. وتمكّن مجرمو الانترنت من دخول نظام الدفع لشركة Home Depot عن طريق بائع من طرف ثالث ثم إطلاق البرمجيات الخبيثة للحصول على بيانات أجهزة نقاط البيع التي تمتلكها الشركة. وكان للاختراق أثر طويل الأجل على الشركة وعلى الشركات الأخرى المرتبطة معها من خلال نقاط البيع. فمنذ عام 2014 تكبّدت الشركة خسائر تقدر بقيمة 300 مليون دولار، بسبب دفعها لتكاليف الضمان للزبائن المتأثرين، والغرامات والأتعاب الأخرى، وإعادة إصدار ملايين البطاقات الجديدة (CEA USA, 2018).

رابعاً: إدارة المخاطر الالكترونية ونماذج التعامل معها

تبرز أهمية إدارة المخاطر الالكترونية كواحدة من أهم المخاطر النظامية التي تواجه الأنظمة الاقتصادية والمالية العالمية، وتمثل إدارة هذا النوع من المخاطر واحدة من التحديات المهمة التي تواجه المؤسسات العامة والخاصة في الآونة الأخيرة وذلك لما لها من آثار بالغة على بقاءها وسمعتها. ويعتبر الأمن الالكتروني سلعة عامة (Public good) ولها آثار خارجية سلبية يمكن أن تنتشر في الأنشطة الاقتصادية على نطاق واسع مما يهدد الاستقرار الاقتصادي والمالي في الدولة،

كما بيّنا ذلك في المحور السابق من الدراسة. ونريد في هذا المحور توضيح كيفية إدارة المخاطر السيبرانية وبناء المنعة ضد هذه الهجمات والتعامل معها.

وباعتبار تعقيد التهديد الالكتروني، لم يعد كافياً تصميم خطة لإدارة المخاطر في المؤسسة مبنية على سناريو أو افتراض "اذا تمت مهاجمتنا" ولكن بالأحرى ان تُبنى على افتراض "عندما تتم مهاجمتنا" أو "كم عدد المرات التي نهاجم فيها" أو "حتى متى نتمكن من الاستمرار في المقاومة" . ولفهم وإدارة المخاطر السيبرانية النظامية، يجب على المؤسسة التشارك مع الموردين (وموردي الموردين) والزبائن والكيانات الأخرى المرتبطة بها فعلياً في تحديد نطاق المخاطر المحتملة والسيناريوهات والمحفزات التي تساعد على وقوع الأحداث السيبرانية النظامية. كما أنه من الضروري تحديد وتقييم أصول البنية التحتية الحيوية المعرضة للخطر في المؤسسة، وسد الثغرات التي قد تُعرّض هذه الأصول للإصابة بالمخاطر وتقييم قدرات ودوافع الجهات الفاعلة في التهديد الالكتروني والتي تستهدف تلك الأصول. ثم بعد ذلك التعاون مع المؤسسات والكيانات الأخرى لمجابهة هذه المخاطر. ويساهم تقييم المخاطر الالكترونية بشكل عام في تعزيز برنامج الأمن الالكتروني من خلال توفير المعلومات المطلوبة لتحديد أولويات أنشطة إدارة المخاطر داخل هذا البرنامج.

المبادئ التي تقوم عليها بناء المنعة ضد المخاطر الالكترونية

يقوم بناء المنعة ضد المخاطر الالكترونية على مجموعة من المبادئ العامة أهمها ما يلي:

1. إقرار المؤسسات بطبيعة التداخل والترابط العالي العالمي وأن تقوم بدورها في تأمين البيئة الالكترونية أو الرقمية الكلية (Digital Environment).
2. قيام الفريق الإداري التنفيذي بالمؤسسة بوضع وتصميم خطط لبناء المنعة ضد المخاطر الالكترونية.
3. أهمية دمج مخاطر الهجمات الالكترونية ضمن إطار المخاطر الكلية التي تواجهها المؤسسة ووفقاً للمبادئ والتعليمات العامة الدولية لبناء المنعة ضد المخاطر السيبرانية.
4. حث المؤسسة لمورديها المعتمدين بتبني المبادئ والتعليمات العامة لمجابهة المخاطر المرتبطة بالهجمات الالكترونية (WEF, 2012).

نموذج النضج في بناء المنعة ضد الهجمات الالكترونية في المؤسسات:

طوّر هذا النموذج المنتدى الاقتصادي العالمي في جنيف في عام 2011 وتمر المؤسسة في هذا النموذج بخمسة مراحل للوصول لمرحلة النضج في بناء المنعة ضد المخاطر الالكترونية على النحو التالي:

المرحلة الأولى وهي مرحلة عدم الإدراك للمخاطر، وترى المؤسسة في هذه المرحلة أن مخاطر الهجمات السيبرانية ليست ذات صلة بعملها ولا تدخل في دائرة المخاطر العامة التي تواجهها المؤسسة. أما المرحلة الثانية فهي مرحلة تكوين رؤى مجزأة أو مفتتة (Fragmented) وتدرك المؤسسة في هذه المرحلة خطورة الارتباط العالمي المفرط في عالم الاتصالات والانترنت ولكنها ذات إدراك محدود في مجال إدارة الهجمات الالكترونية. فالمؤسسة لها طريقة منعزلة ومجزأة في مواجهة هذا النوع من المخاطر. وتبدأ المؤسسة في المرحلة الثالثة في إدارة المخاطر الالكترونية من أعلى إلى أسفل Top-Down بواسطة المدير التنفيذي للمؤسسة والذي يشرع في وضع برامج للاستجابة لهذه المخاطر من أعلى إلى أسفل ولكنه لا يرى أن إدارة هذا النوع من المخاطر يعطي المؤسسة ميزة تنافسية في الاسواق. والمرحلة الرابعة هي مرحلة تغلغل إدارة المخاطر Pervasive وفيها تضع القيادة يدها على إدارة المخاطر الناجمة عن الهجمات الالكترونية من خلال تطوير السياسات والأطر وتحديد المسئوليات وآلية الإفصاح عنها مع الفهم التام لها ولارتباطات الأطراف الأخرى بها. والمرحلة الأخيرة هي مرحلة التشبيك Networked وتكون المؤسسة في هذه المرحلة مرتبطة ارتباطاً وثيقاً بالمؤسسات المماثلة والشركاء وتتبادل المعلومات معهم، وتعمل معهم بصورة يومية على خفض آثار هذه الهجمات. ويكون الأفراد بالمؤسسة على دراية تامة بتلك المخاطر وتكون المؤسسة رائدة في إدارة هذا النوع من المخاطر (WEF, 2015, 2017).

إطار بناء المنعة ضد المخاطر الالكترونية

طوّر المنتدى الاقتصادي العالمي (WEF) اطاراً لبناء المنعة ضد المخاطر الالكترونية كما هو مبيّن في الشكل رقم (1). ويساعد هذا الإطار المؤسسات على فهم المخاطر الالكترونية وتحليلها وإدماجها ضمن خططها الاستراتيجية وذلك للمساعدة في اتخاذ القرار الملائم لمجابهة هذه المخاطر وبناء المنعة ضدها، بالإضافة إلى إعداد الميزانيات وإتاحة الموارد المناسبة لذلك. وتتكون العناصر

الأساسية لإطار بناء المنعة ضد المخاطر الالكترونية من التهديدات والقابلية للإصابة (أو الثغرات) والقيم التي في خطر والاستجابات.

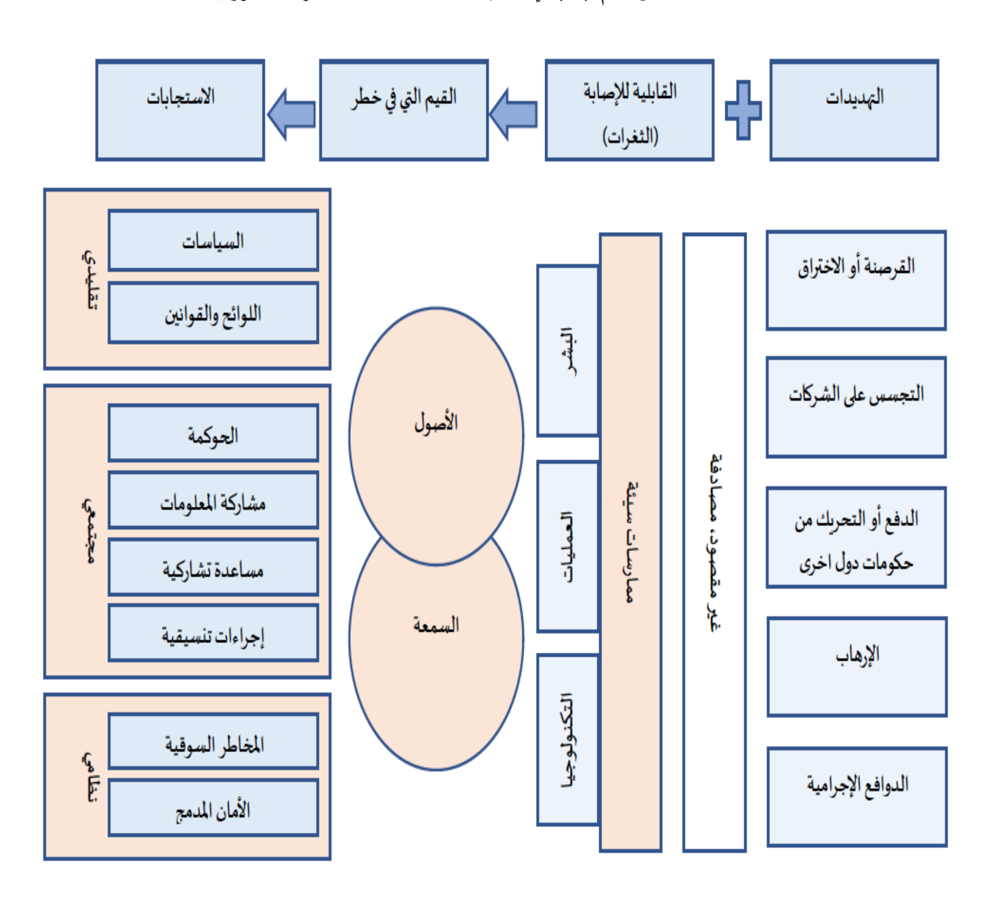
ويقوم إطار بناء المنعة ضد المخاطر الالكترونية (في الشكل رقم (1)) على أن التهديدات والثغرات (القابلية بالإصابة) تنعكس على القيم التي في الخطر والتي تستدعي الاستجابات لمجابهة هذه المخاطر. وتعتبر المخاطر الالكترونية مشكلة تجارية ذات جوانب تقنية. ويُعرّف هذا الإطار المخاطر الالكترونية على أنها مزيج من احتمالية وقوع حادث داخل نطاق نظم المعلومات في المؤسسة وتأثير هذا الحادث على أصولها الملموسة وغير الملموسة. ويمكن أن تؤثر المخاطر السيبرانية على جميع مجالات عمل المؤسسة وأن تتأثر بها بتضخيمها أو بالحد منها، بل وقد تتعداها الى مؤسسات وأجزاء أخرى من سلسلة القيمة في الإنتاج الاقتصادي. والشكل رقم (1) يوضح الإطار الذي طوّره المنتدى الاقتصادي العالمي (WEF) لبناء المنعة لمجابهة المخاطر التكنولوجية

وتحدث آثار الحادث السيبراني في المؤسسة في هذا الإطار، بسبب فقدان واحد أو أكثر من خصائص الأصول النوعية – سواء كان ذلك بفقدان السرية أو النزاهة أو التوافر أو المساءلة. ويشير تقييم التهديدات والقابلية للإصابة (أو الثغرات) (vulnerabilities) إلى تقييم احتمالية وقوع حادث سيبراني ويُفضل أن يكون هذا التقييم كميًا، وفي حالة عدم توفر ذلك يُجرى تقييم نوعي باستخدام الفئات "منخفض / متوسط / مرتفع" لتحديد أولويات المخاطر. وتشتمل التهديدات في هذا الإطار على القرصنة أو الاختراق والتجسس والهجوم المدفوع من قبل حكومات قومية والإرهاب وجرائم التخريب بالإضافة الى الزبائن الساخطون، الأخطاء البشرية، الموردين، أعمال الشركاء، والعملاء من داخل المؤسسة والقوة القهرية. أما الثغرات (أو القابلية للإصابة) فتشمل الناس والثقافة والعمليات والأنظمة التكنولوجية والبنية التحتية.

وتنقسم الاستجابات للمخاطر الالكترونية إلى ثالثة أنواع هي الاستجابات التقليدية والمجتمعية والنظامية، فالاستجابات التقليدية تتمثل في السياسات أو المبادرات واللوائح والقوانين التي تقوم بها المؤسسة. وتشير الاستجابات المجتمعية إلى مشاركة المعلومات مع الأطراف المجتمعية الأخرى والمساعدات التشاركية والإجراءات التنسيقية والحوكمة. أما الاستجابات النظامية فهي المخاطر السوقية والأمان المدمج. والجدول رقم (1) يعطي أمثلة توضيحية للمخاطر الالكترونية في

إطار بناء المنعة ضدها وما يرتبط بهذه المخاطر من الأصول التي في الخطروالخسائر والتهديدات وقابلية للإصابة بها.

الشكل رقم (1): إطار بناء المنعة ضد المخاطر الالكترونية



المصدر: المنتدى الاقتصادي العالمي (WEF, 2017)

الجدول رقم (1): أمثلة توضيحية على المخاطر في إطار بناء المنعة وما يرتبط بها من الأصول والخسائر والتهديدات والقابلية للإصابة

المخاطرة	الأصول التي في خطر	الخسائر	التهديدات	القابلية للإصابة	الآثار والقياس الكمي
فقدان النزاهة والمساءلة في البيانات المالية	المعلومات المالية أو الأنظمة: على سبيل المثال أوامر التحويل	فقدان النزاهة والمساءلة	حدوث جريمة داخلية	العمليات: نقص التحكم في التغيير (المزدوج) يُمكّن الموظف من التلاعب في نظم البيانات المالية	- الخسائر المباشرة الناتجة عن الاحتيال المالي مطروحًا منها استرداد التأمين - التكلفة المباشرة للتحقيق في الحادث (الموارد الداخلية والخارجية المستخدمة) - مخاطر السمعة، والتأثير على المبيعات ، التجديدات والحصة السوقية وسعر السهم - رسوم الغرامات والاتعاب
فقدان سرية بيانات العميل	بيانات العميل، سمعة المؤسسة	فقدان السرية	هجوم التصيد من منظمات اجرامية	الانسان: ارسال بيانات العملاء عبر البريد الإلكتروني	- التكلفة المباشرة للتحقيق في الحادث (الموارد الداخلية والخارجية). - التكلفة لكل سجل للعميل الاتصالات ومراقبة سرقة الهوية - مخاطر السمعة، التأثير على المبيعات، التجديدات وحصة السوق و / أو المشاركة السعر. - رسوم العقوبات التنظيمية والغرامات.
فقدان توافر أنظمة الإنتاج	مخرجات الانتاج والمخرجات الإرادية المحتملة من هذا الانتاج	توفر أو اتاحة الخدمة	هجوم الحرمان من الخدمة الموزعة (DDoS) بسبب الاختراق أو لتمكين الاحتيال	التكنولوجيا: عدم وجود ضوابط للحد من تأثير هجوم DDoS أو التعافي عقب هذا هجوم	- التكلفة المباشرة للتحقيق في الحادث (الموارد الداخلية والخارجية). - تكلفة انقطاع الإنتاج مثلا عقوبة خرق اتفاقيات مستوى الخدمة، وفقدان الإيرادات بسبب فقدان المعاملات أو الغرامات، العقوبات أو الدعاوى القضائية بسبب فقدان الصفقات التجارية - التأثير على السمعة وفقدان الأعمال المستقبلية. - مخاطر السمعة، التأثير على المبيعات، التجديدات وحصة السوق و / أو المشاركة السعرية

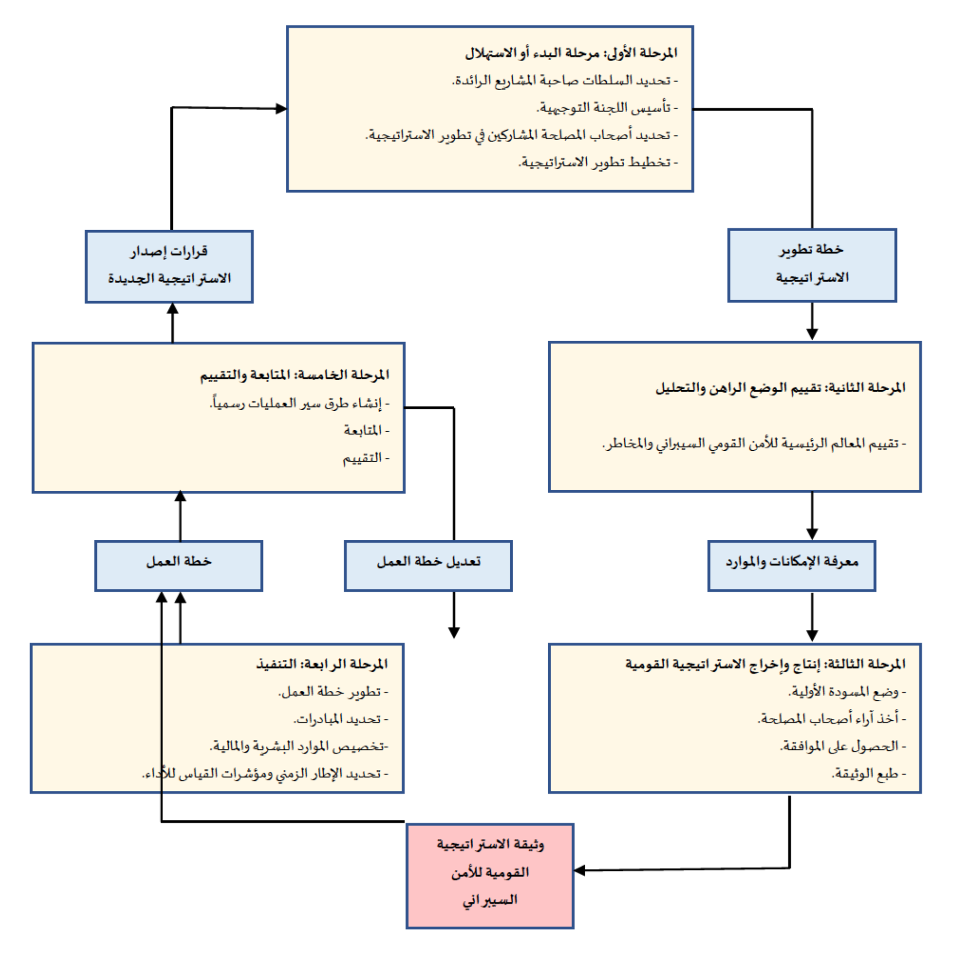
المصدر: المنتدى الاقتصادي العالمي (WEF, 2017).

تطوير استراتيجية وطنية للأمن السيبراني

الشكل رقم (2) يقدم لمحة عامة عن المراحل المختلفة في تطوير الاستراتيجية الوطنية للأمن السيبراني وفقاً لمقترح مشترك من عدة جهات دولية تتضمن وحدة الاتصالات في الأمم المتحدة والبنك الدولي وغيرها. وتشتمل هذه الاستراتيجية المقترحة على خمسة مراحل وهي: المرحلة الأولى وهي مرحلة البدء أو الاستهلال التي يتم فيها تحديد السلطات أو الجهات صاحبة المشاريع الرائدة في الاستراتيجية وتأسيس اللجنة التوجيهية وتحديد أصحاب المصلحة المشاركين في

تطوير الاستراتيجية وتخطيط تطويرها. والمرحلة الثانية هي مرحلة تقييم الوضع الراهن والتحليل والثالثة هي إنتاج وإخراج الاستراتيجية من خلال وضع المسودة الأولية وأخذ آراء أصحاب المصلحة والحصول على الموافقة وطبع الوثيقة. أما المرحلة الرابعة فهي مرحلة التنفيذ وتشتمل على تطوير خطة العمل وتحديد المبادرات وتخصيص الموارد البشرية والمالية وتحديد الإطار الزمني ومؤشرات القياس للأداء. وفي المرحلة الأخيرة تتم المراقبة والتقييم من خلال إنشاء طرق سير العمليات رسمياً والمتابعة والتقييم (UN-ITU et al, 2018).

الشكل رقم (2): دورة حياة الاستراتيجية القومية للأمان السيبراني (الأمم المتحدة بالاشتراك مع البنك الدولي وآخرين)



المصدر: (United Nation- International Telecommunication Unit (ITU) et al., 2018)

إجراءات إدارة المخاطر الالكترونية

تُتخذ إجراءات إدارة المخاطر الالكترونية بعد تحديد ومراجعة احتمالية وقوعها وآثارها. ويجب تقييم هذه الإجراءات من قبل الإدارة التنفيذية قبل البدء في تنفيذها. وتتضمن هذه الإجراءات الأنواع التالية:

أ. إجراءات تخفيف المخاطر الالكترونية: يمكن تخفيف هذه المخاطر من خلال استخدام الضوابط التقنية والإدارية والمادية (أو البدنية) والتنظيمية كما هو مبيّن في الأمثلة التالية: (1) ضوابط المخاطر التي تستهدف الناس والثقافة من خلال تدريب الموظفين، أو حملات التوعية. (2) ضوابط المخاطر التنظيمية والإجرائية من خلال ضبط الأحكام تعاقدية والسياسات والحوكمة والتشريعات وتبادل المعلومات الذكية عبر الصناعات أو المساعدات المتبادلة والردود المنسقة (وتشمل هذه الفئة ضوابط المخاطر الإدارية مثل ضبط مخزونات الأصول وتصنيف المخاطر). (3) ضوابط المخاطر الفنية: من خلال تعزيز جدار الحماية الالكترونية وقدرات الكشف للتهديدات وقدرات الاستجابة أو الاستعادة للنظام بعد الهجوم وضوابط الوصول المادي للأنظمة.

ب.إجراءات نقل – يتم نقل المخاطر، على سبيل المثال عن طريق عقود التأمين في أسواق المخاطر.

ج. إجراءات القبول - المخاطر التي تكون طفيفة أو لا يمكن أن يتم تخفيفها بطريقة فعالة، يمكن قبولها.

د. إجراءات التجنب - المخاطر التي تقع خارج نطاق تحمل أو تحكم المؤسسة يجب تجنبها (على سبيل المثال، منتج تم سحبه من السوق) (WEF، 2017).

خامساً: واقع وأهمية المخاطر الالكترونية على المستوى العالمي

في ظل الثورة الصناعية الرابعة، أدى التقارب التكنولوجي العالمي الى تبديد الفواصل بين العالم المادي والرقمي والبيولوجي بطرق أثرت بعمق على الناس والاقتصادات في جميع أنحاء العالم. كما أدت التقنيات الجديدة في نظم المعلومات الى ترابط غير مسبوق بين بلدان العالم المختلفة مما

زاد من مخاطر الهجمات الإلكترونية الخبيثة. ونظرا لطبيعة تعقيد بيئة المخاطر الالكترونية النظامية لم يعد بمقدور أي كيان أو مؤسسة معينة مواجهة المخاطر الإلكترونية بمفردها من خلال الأنظمة أو الشبكات التي تسيطر عليها. وذلك بسبب عدم توفر السلطات والإمكانات والطاقات الكافية التي تمكّنها من مجابهة نطاق أو سرعة تطوّر الخطر الالكتروني.

يتناول هذا المحور من الدراسة واقع وأهمية المخاطر الالكترونية على المستوى العالمي بالتركيز على الفترة 2015-2018 واستعراض أهمية المخاطر النظامية الالكترونية التي تواجه القطاع المالي العالمي في الآونة الأخيرة والدول الأكثر عرضة لهذه الهجمات، ومن ثمّ تحليل واقع الهجمات الالكترونية وفقاً للأصناف التالية: البرمجيات الخبيثة Malware، البرمجيات الخبيثة المطالبة بالفدية Ransomware، تهديدات الشبكة Web Threats، تهديدات البريد الالكتروني Email Threats، التصيّد Phishing، والاحتيال Spam، التعرض للإصابة بالمخاطر الالكترونية Vulnerabilities، الهجمات الاستهدافية Targeted Attacks، وتهديدات الهاتف المحمول Mobile Threats.

أهم المخاطر النظامية التي واجهت النظام المالي العالمي في الفترة 2018-2017

يعتبر القطاع المالي من أكبر القطاعات المستهدفة بالهجمات الالكترونية الخبيثة نسبة لدوره في الوساطة المالية واعتماده على نظم المعلومات في أداء مهامه. ويمكن أن تؤثر الهجمات السيبرانية على المؤسسات المالية من خلال تأثيرها على أمن المعلومات من جانب السرية والنزاهة والتوافر. ونركّز في هذه الدراسة على القطاع المالي لعدة أسباب أهمها: أن هذا القطاع يمثّل أسرع وأقوى منظومة لإرسال الاشارات signals التي تنذر بوجود خلل رئيسي في المنظومة الاقتصادية في الدولة أو بوشك حدوث أزمة أو ازدياد حجم المخاطر المالية الجزئية وتفشي الصدمات الداخلية والخارجية على حد سواء، مع انتشار التأثيرات التراكمية لهذا القطاع الى بقية القطاعات المالية والحقيقية الأخرى.

تعتبر المخاطر والهجمات السيبرانية وخروق خصوصية المعلومات من أكبر التحديات التي تواجه هذا القطاع. فمع زيادة الخدمات المالية عبر الهاتف المحمول والاستعانة بالمصادر الخارجية (outsourcing) في تقديم الخدمات المالية تزداد مخاطر حماية المستهلك وغسيل الأموال وتنظيم القطاع المالي غير المصرفي. وتُمثل الهجمات الالكترونية الخبيثة أعظم المخاطر التي تواجه هذا القطاع وذلك بسبب ازدياد تواترها وعدم إمكانية التنبؤ بها وانتشار تأثيرها القطاعي المحتمل ووجود الثغرات في إدارة مخاطرها. وأشارت دراسات صندوق النقد الدولي الى أن أهم المخاطر التي تواجه الاستقرار المالي العالمي في العام في عام 2018 وما بعده تتمثّل في المخاطر السيبرانية، الجغرافيا السياسية، آثار القوانين الجديدة، خروج بريطانيا من اليورو، وتغيرات السياسة النقدية الأمريكية. وقد جاءت المخاطر السيبرانية في طليعة هذه المخاطر التي تواجه النظام المالي العالمي وفقاً لاستطلاع الرأي العالمي في نهاية عام 2017، حيث تصدّر هذا النوع من المخاطر القائمة العالمية لنسبة 78 % من المشاركين في الاستطلاع، وتلي ذلك الجغرافيا السياسية بنسبة 69 % كما هو موضح في الجدول رقم (2).

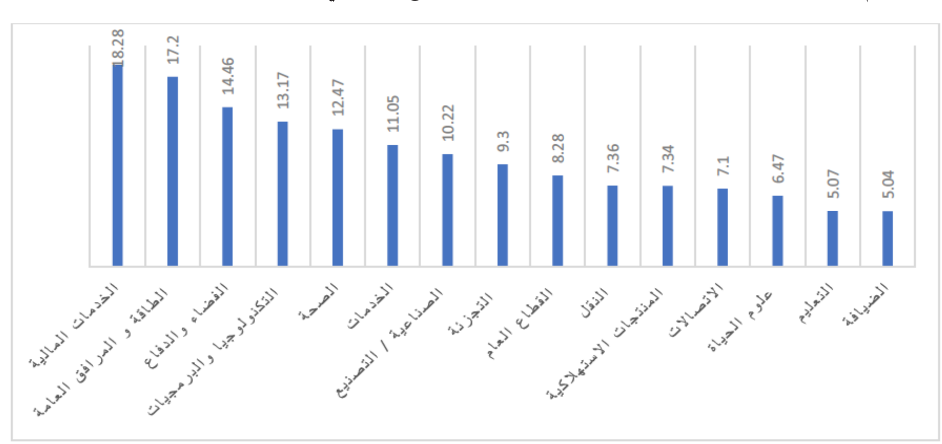
الجدول رقم (2): ترتيب أهم 5 مخاطر تواجه النظام المالي العالمي لعام 2018 وما بعده.

الخطر	ترتيب الخطر وفقا للمستجيبين في الربع الثالث من عام 2017	النسبة المئوية في الربع الثالث من عام 2017	النسبة المئوية في الربع الأول من عام 2017
المخاطر السيبرانية	1	78	71
الجغرافيا السياسية	2	69	52
آثار القوانين الجديدة	3	45	40
خروج بريطانيا من اليورو	4	38	34
تغيرات السياسة النقدية الأمريكية	5	25	29

المصدر: (DTCC Systemic Risk barometer 2017Q1 and IMF (2018)

وازدادت في الآونة الأخيرة اعداد البرمجيات الخبيثة الموجهة للقطاع المالي Financial Trojan والتي من أشهرها Trojan horse، وهو برنامج خبيث يضلل الضحية عن قصده الأساسي وذلك لألحاق الضرر به. وقد ظهر نوع جديد من فيروسات Emotet خلال عام 2017 والتي تحاول استخدام بعض النوافذ المعينة لتتجنب الاستكشاف بواسطة نظم الحماية في أنظمة المؤسسات المالية. وتتفاوت التكاليف المالية للهجمات الالكترونية وفقاً لنوع النشاط الاقتصادي للمؤسسات الاقتصادية، فترتفع تكلفة الجريمة الالكترونية في قطاع الخدمات المالية وقطاع الطاقة والمرافق العامة وقطاع الفضاء والدفاع. والشكل رقم (3) يوضح متوسط التكلفة السنوية للجريمة السيبرانية لعينة من الشركات العالمية بملايين الدولارات. ويبيّن الشكل أن التكلفة المالية للجرائم الالكترونية في قطاع الخدمات المالية هي الأعلى عالمياً مقارنة ببقية القطاعات الأخرى ويليها في ذلك قطاع الطاقة والمرافق العامة.

الشكل رقم (3): متوسط التكلفة السنوية للجريمة السيبرانية حسب القطاع الاقتصادي لعينة من الشركات العالمية بملايين الدولارات



المصدر: Ponemon Institute LLC and Accenture (2017)

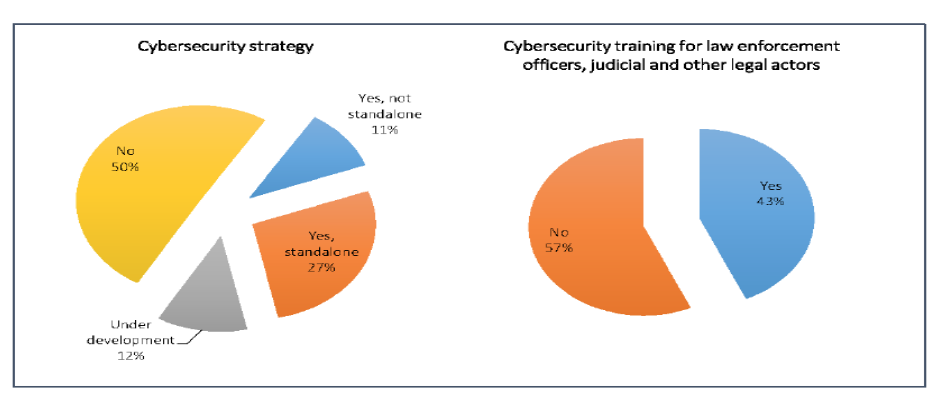
أوضاع الأمن السيبراني العالمي وفقاً لدليل الأمن السيبراني العالمي (GCI – Global Cyber security Index)

اهتمت هيئة الأمم المتحدة بالأمن الالكتروني لما له من آثار عالمية بالغة على الدول والأفراد والأنشطة الاقتصادية. وقد صمّمت وحدة الاتصالات العالمية في الأمم المتحدة International

ITU (Telecommunication Unit) دليل خاص لهذا الغرض وهو دليل الأمن السيبراني العالمي (GCI – Global Cyber security Index) والذي يقيس مستوى التزام الدول المختلفة بالأمن الالكتروني ويوفر المعلومات الاساسية لتحليل ومقارنة أداء الدول العالمية من خلال خمسة ركائز رئيسية وهي العوامل القانونية والفنية والترتيبات التنظيمية وبناء القدرات والتعاون ويُمكن تفسير هذه الركائز على النحو التالي:

1. القانون: يقاس على أساس وجود مؤسسات وأطر قانونية تتعامل مع الأمن الالكتروني والجريمة الالكترونية في الدولة.
2. التقنية: تقاس على أساس وجود المؤسسات والأطر التقنية التي تتناول الأمن الالكتروني في الدولة.
3. التنظيم: يقاس على أساس وجود مؤسسات واستراتيجيات تنسق سياسات تطوير الأمن الالكتروني على المستوى الوطني.
4. بناء القدرات: يقاس على أساس وجود برامج البحث والتطوير والتعليم والتدريب للمهنيين المعتمدين ووكالات القطاع العام التي تعزز بناء القدرات في الدولة.
5. التعاون: يقاس على أساس وجود شراكات وأُطر تعاونية وشبكات لتبادل المعلومات بين الدولة والدول الأخرى.

الشكل رقم (4): توفر استراتيجية للأمن السيبراني ومستوى الالتزام الدولي بالتدريب



المصدر: تقرير الأمن السيبراني (2017).

يبيّن الشكل رقم (4) أن نصف دول العالم لا تتوفر لديها استراتيجية للأمن السيبراني وأن نسبة 12% منها لديها استراتيجية في طور التطوير و27% منها لديها استراتيجيات ولكنها ليست مستقلة و11% فقط تتمتّع باستراتيجيات مستقلة (Standalone). مما يدل على أن العديد من دول العالم لا زالت تفتقر لهذه الاستراتيجيات. كما يوضح الشكل رقم (4) أن أكثر من نصف دول العالم (نسبة 57% منهم) لا توفر تدريب للعاملين في مجالات تطبيق القانون والقضاء والتشريع المرتبط بالأمن الالكتروني.

والجدول رقم (3) يوضح ترتيب دول العالم وفقاً للدليل العالمي للأمن السيبراني وقد تصدّرت سنغافورة وأمريكا القائمة وتليها ماليزيا وعُمان واستونيا وموريشيوس واستراليا وجورجيا وفرنسا وكندا. كما يوضح الجدول أداء هذه الدول في المؤشرات الفرعية للدليل وهي القانون والتقنية والتنظيم ورفع القدرات والتعاون. وقد احتلت عُمان المرتبة الرابعة عالمياً في الدليل الكلي، كما أنها تميّزت عالمياً في جانب القانون ورفع القدرات.

الجدول رقم (3): الدول العشرة الأعلى التزاماً باستراتيجية الأمن السيبراني

Top ten most committed countries, GCI (normalized score)

الدولة	قيم الدليل GCI Score	القانون Legal	التقنية Technical	التنظيم Organizational	رفع القدرات Capacity Building	التعاون Cooperation
سنغافورة	0.92	0.95	0.96	0.88	0.97	0.87
امريكا	0.91	1	0.96	0.92	1	0.73
ماليزيا	0.89	0.87	0.96	0.77	1	0.87
عمان	0.87	0.98	0.82	0.85	0.95	0.75
استونيا	0.84	0.99	0.82	0.85	0.94	0.64
موريشص	0.82	0.85	0.96	0.74	0.91	0.70
استراليا	0.82	0.94	0.96	0.86	0.94	0.44
جورجيا	0.81	0.91	0.77	0.82	0.90	0.70
فرنسا	0.81	0.94	0.96	0.60	1	0.61
كندا	0.81	0.94	0.93	0.71	0.82	0.70

المصدر: تقرير الأمن السيبراني العالمي (2017).

مجالات وأنواع الهجمات الالكترونية على الأنشطة الاقتصادية في العالم خلال الفترة 2015-2018

أصبحت المخاطر والتهديدات الالكترونية تطوّر بمرور الوقت وتأتي من جماعات إجرامية متطورة وتحدث حالات اختراق الأمن الالكتروني في العادة عبر الشبكات بسبب وجود الثغرات الأمنية. وتتمثل أهم أنواع الهجمات الالكترونية في البرمجيات الخبيثة والبرمجيات الخبيثة المطالبة بالفدية وتهديدات الشبكة وتهديدات البريد الالكتروني والتصيد الالكتروني (Phishing) والاحتيال (Spam)، والهجمات الاستهدافية الاستخبارية وتهديدات الهاتف المحمول وسيتم تفصيلها في الفقرات التالية.

1. نشاط البرمجيات الخبيثة Malware

وفقاً لتقرير (2018) ISTR فإن أعلى مجالات الجريمة الالكترونية نمواً في عام 2017 هو أنشطة التعدين للنقود الالكترونية أو العملات المشفرة (Coin Mining of Crypto Currencies) مثل البتكوين (Bitcoin) على الانترنت حيث اكتشفت برامج مضادات الفيروسات زيادة في هذه الانشطة تُقدّر بنسبة 8500%. وارتفعت معدلات الفيروسات المستهدفة للفدية Ransomware بنسبة 40% في نفس العام ويرجع ذلك في المقام الأول الى نشاط فيروس (Ransom Wannacry) . كما عاد إلى الظهور فيروس Emotet (Trojan Emotet)) كمهدد جديد للقطاع المصرفي في أواخر عام 2017. وازدادت عدد الاكتشافات لهذا الفيروس الخبيث بنسبة 2000% في الربع الأخير من ذلك العام، كما ازداد عدد تنزيلات البرامج الخبيثة المستهدفة للقطاع المالي بنسبة 92%. ويرجع معظم النمو في الأنواع الجديدة من البرمجيات الضارة في عام 2017 إلى فيروس Kotver Trojan والتي مثلت حوالي 88% منها.

2. نشاط البرمجيات الخبيثة المطالبة بالفدية Ransomware

ازداد عدد النسخ الجديدة من البرمجيات الخبيثة المطالبة بالفدية بنسبة 45% في عام 2017، وذلك من 241.021 برمجية في عام 2016 الى 350.496 في عام 2017.

كما ازداد عدد الهجمات التي تم اكتشافها وإيقافها بنسبة 41% في نفس العام. وانخفض متوسط قيمة الفدية المطلوبة من قبل مجرمي الانترنت من 1071$ في عام 2016 إلى 522$ في عام 2017، كما هو موضوح بالجدول رقم (4).

الجدول رقم (4): متوسط الفدية النقدية المطلوبة

السنة	الفدية المطلوبة بالدولار
2014	372
2015	294
2016	1071
2017	522

المصدر: ISTR Report (2018)

3. تهديدات الشبكة Web Threats

ارتفعت تهديدات الشبكة بنسب عالية في عام 2017، فقد وُجد أن 1 من كل 13 محدد من محددات مواقع المعلومات على الانترنت في المدخل (URLS) خبيث أو ضار بالمستخدم، بعد أن كانت هذه النسبة تساوي 1 في كل 20 في عام 2016. ومع تقدم عام 2017، ازدادت عدد الهجمات التي تم كشفها وإيقافها بسبب ارتفاع نشاط التعدين عن العملات المشفرة Crypto Currencies. وقد تم إيقاف ما يعادل 611.141 هجمة في المتوسط يومياً. وأظهر التصنيف العالمي أن أكثر المواقع الالكترونية التي يتم استغلالها من قبل مجرمي الانترنت هي مواقع البرمجيات الضارة بنسبة 15.9 % ومواقع Dynamics DNS وهي مواقع للتحديث الذاتي في الانترنت للنطاق والاسم والنظام (DNS) Domain, Name, System ومواقع التكنولوجيا والأعمال التجارية، كما هو موضح بالجدول رقم (5).

الجدول رقم (5): تصنيف أكثر المواقع الالكترونية التي تم استغلالها من قبل مجرمي الانترنت

الترتيب	الفئة أو النشاط	2016 (%)	2017 (%)	الفرق النسبي
1	البرمجيات الخبيثة	1.4	15.9	14.5
2	ديناميكي (DNS)	0.1>	13.2	13.2
3	التكنولوجيا	20.7	11.5	9.2-
4	الأعمال التجارية	11.3	7.5	3.7-
5	السكن	7.2	6.9	0.3-
6	القمار	2.8	6.7	3.9
7	الصحة	5.7	4.8	0.9-
8	التسوق	4.2	3.8	0.3-
9	التعليم	4.1	3.1	1.0-
10	السفر	3.6	2.8	0.8-

المصدر: (2018) ISTR Report.

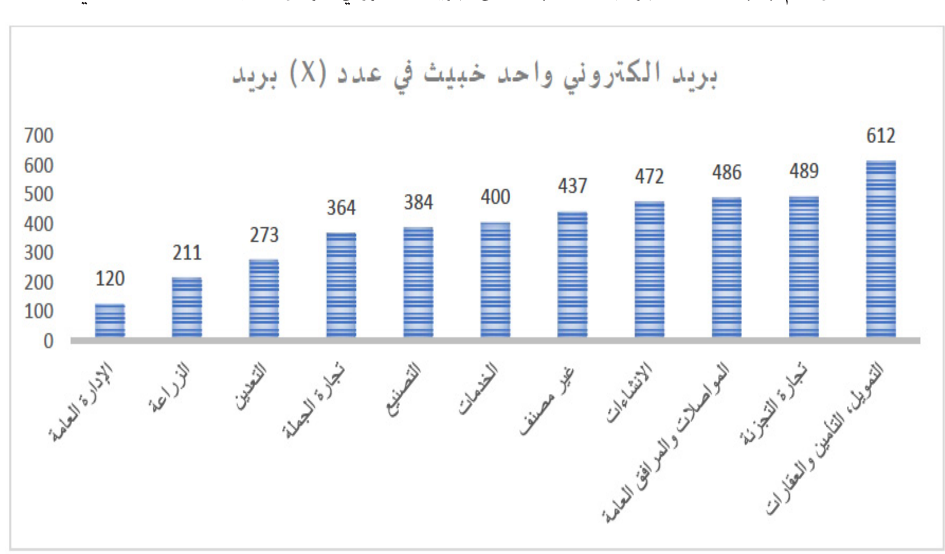
4. تهديدات البريد الالكتروني Email Threats

انخفضت عدد البرمجيات الخبيثة في البريد الالكتروني من 1 في كل 131 بريد في عام 2016 إلى 1 في كل 412 بريد في عام 2017. وقد أرسلت فيروسات Necurs botent الخبيثة حوالي 15 مليون بريد الكتروني ضار في عام 2017. وتأثرت شهرياً حوالي 7710 مؤسسة عالمية باحتيال يعرف باسم (Business Email Compromise) BEC Scam والتي نتجت عنها أضراراً مادية بليغة. وعلى مستوى الأنشطة الاقتصادية، جاءت أعلى معدلات البريد الالكتروني الخبيث في قطاع الإدارة العامة حيث بلغت معدل واحد بريد الكتروني في كل 120 بريد، تليها قطاع الزراعة بمعدل واحد في كل 211 بريد كما هو موضح في الشكل رقم (5).

وتفاوتت معدلات البرمجيات الضارة في محددات مواقع المعلومات على الانترنت (URLS) وفقاً الأنشطة الاقتصادية وتصدّر قطاع الانشاءات قائمة القطاعات الاقتصادية في نسب البريد الالكتروني الخبيث المرسل حيث احتوت نسبة 27.2% من الروابط المرسلة في هذا

القطاع على برنامج خبيث بدلاً عن مرفقات عادية. ويلي ذلك قطاع الزراعة بمعدل 25% من الروابط المرسلة.

الشكل رقم (5): معدلات البرمجيات الخبيثة على البريد الالكتروني المرسل حسب النشاط الاقتصادي



المصدر: 2018) ISTR Report)

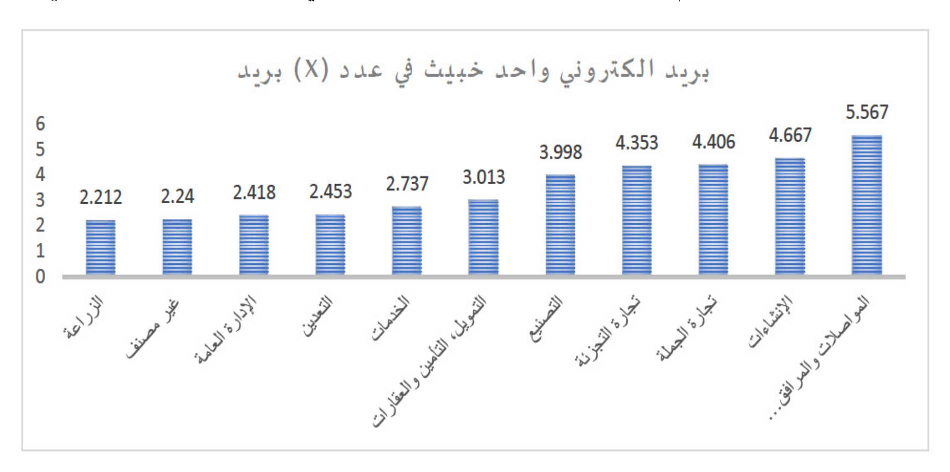
5. التصيد الالكتروني Phishing

ازدادت في الآونة الأخيرة معدلات التصيّد الالكتروني Phishing على مستخدمي الانترنت فبلغت معدل بريد الكتروني خبيث واحد في كل 2212 بريد في القطاع الزراعي كأعلى معدل إلى بريد واحد في كل 5567 في قطاع المواصلات والمرافق العامة كأدنى معدل كما في الشكل رقم (6-A).

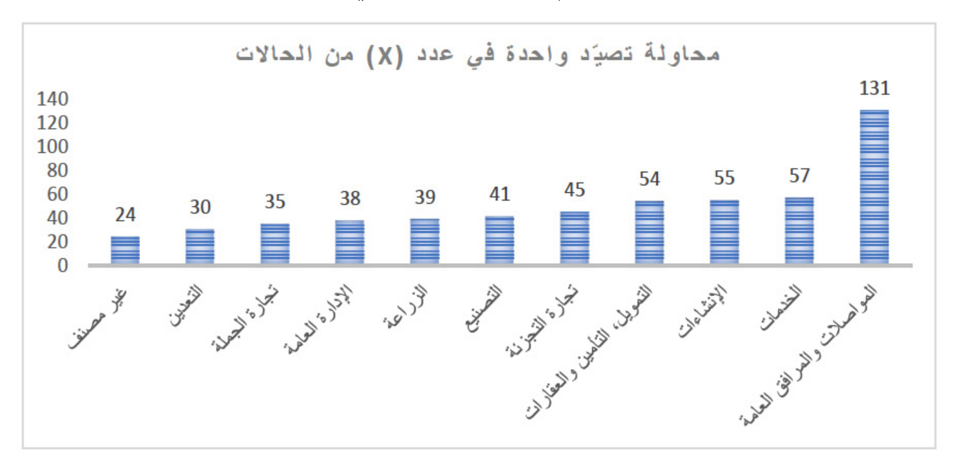
ويوضح الشكل رقم (6-B) نسب مستخدمي البريد الالكتروني الذين وقعت عليهم محاولات التصيد حسب الأنشطة الاقتصادية، والتي تتراوح بين وقوع محاولة تصيّد واحدة في كل 30 بريد الكتروني في قطاع التعدين كأعلى معدل إلى محاولة واحدة في كل 131 بريد الكتروني في قطاع المواصلات والمرافق العامة. والجدول رقم (6) يوضح الترتيب العالمي للدول حسب الإصابة بالتصيّد

على الانترنت. واحتلت جنوب أفريقيا المرتبة الأولى عالمياً في هذا الترتيب بمعدل محاولة تصيد واحدة في كل 785 بريد الكتروني. تليها هولندا بمعدل محاولة واحدة في كل 1298 بريد الكتروني. وقد ضمت قائمة الدول العشرة في هذا التصنيف كل من: ماليزيا، المجر، البرتغال، النمسا، تايوان، البرازيل، اندونيسيا وسنغافورة.


الشكل رقم (6-A): معدلات التصيد الالكتروني حسب النشاط الاقتصادي



الشكل رقم (6-B): مستخدمو البريد الالكتروني الذين وقعت عليهم محاولات التصيد حسب الأنشطة الاقتصادية



المصدر: ISTR Report (2018)

الجدول رقم (6): التصيّد على الانترنت حسب الدولة

الترتيب	الدولة	حالة واحدة لكل (X) بريد
1	جنوب أفريقيا	785
2	هولندا	1.298
3	ماليزيا	1.359
4	المجر	1.569
5	البرتغال	1.671
6	النمسا	1.675
7	تايوان	1.906
8	البرازيل	2.117
9	اندونيسيا	2.380
10	سنغافورة	2.422

المصدر: ISTR Report (2018).

6. البريد الالكتروني المحتال Spam

وازدادت معدلات الاحتيال الالكتروني (Spam) بنسبة 1.2% في عام 2017، وارتفع معدلات النمو الكلي للاحتيال في البريد الالكتروني خلال الفترة 2015 -2017 من نسبة 52.7% في عام 2015 إلى نسبة 54.6% في عام 2017. والشكل رقم (7) يوضح معدلات البريد الالكتروني المحتال (Spam) حسب النشاط الاقتصادي.

الشكل رقم (7): معدلات البريد الالكتروني المحتال(Spam) حسب النشاط الاقتصادي (نسبة مئوية)



المصدر: ISTR Report (2018)

وارتفع عدد حالات التعرض للإصابة بالمخاطر السيبرانية بنسبة 13 % في عام 2017، فبلغ العدد الكلي للحالات المفصح عنها 8718 حالة بعد أن كانت 7692 في عام 2016. وتباينت مستويات التعرض للمخاطر السيبرانية وفقاً لنوع متصفح الانترنت فارتفعت هذه النسبة في متصفح سفاري Apple Safari بنسبة 14% في عام 2017، وانخفضت في كل من فيرفوكس Fairfox بنسبة 29 % و Edge and Internet Explorer بنسبة 23%، وفي Google Chrome بنسبة 9 %.

7. الهجمات الاستهدافية Targeted Attacks

يمثّل جمع المعلومات الاستخبارية (Intelligence) نحو 90 % من جملة الهجمات الاستهدافية والتي تمارسها بعض الدول والمجموعات السياسية ويقصد منها التجسس وجمع المعلومات لأغراض عسكرية وسياسية وصناعية ومالية. واستخدمت نسبة 71 % من هذه المجموعات وسائل البريد الالكتروني التصيدية الاحتيالية (Spear Phishing Emails) كوسيلة أساسية للهجوم ونقل العدوى. وقد كانت الولايات المتحدة هي الدولة الأكثر استهدافاً في الثلاث سنوات الماضية وواجهت جملة 27 % من أنشطة الهجمات الاستهدافية في العالم. وارتفعت عدد المؤسسات المتضررة من الهجمات الاستهدافية بنسبة 10 % في عام 2017. وارتفع عدد المجموعات الاستهدافية المهاجمة الجديدة التي تم اكتشافها من 87 مجموعة في عام 2015 الى 140 مجموعة في عام 2017. وتمثّلت دوافع المجموعات الاستهدافية في جمع المعلومات الاستخبارية بنسبة تبلغ حوالى 90 %، والتشويش والإرباك والأهداف المالية بنسب تتراوح بين 10-11 %).

8. تهديدات الهاتف المحمول Mobile Threats

ازدادت أنواع البرمجيات الخبيثة الجديدة التي تم اكتشافها في الهواتف المحمولة بنسبة 54 % بين عامي 2016 و2017، وذلك من عدد 17.214 في عام 2016 إلى 26.579 في عام 2017. وقد تمكّنت هذه البرمجيات الخبيثة من تسريب معلومات خاصة بالضحية تشمل أرقام الهواتف (63 %)، وأماكن الاشخاص (37 %). وكان أهم مصدر من مصادر البرامج الخبيثة في الهاتف المحمول هو المتاجر الخارجية ذات التطبيقات الخبيثة (Third-Party apps

Store Malware) وبنسبة 99.9 %.

سادساً: تحليل أوضاع المخاطر الالكترونية في دول مجلس التعاون الخليجي

نتناول في هذا الجزء من الدراسة واقع وأهمية المخاطر الالكترونية في دول مجلس التعاون الخليجي، فنستعرض أنواع الهجمات التي تتعرض لها دول المجلس ونحلل خصوصية هذه الهجمات في استهدافها لقطاع النفط والقطاع المالي بصورة رئيسية. وقد تضمنت الهجمات على القطاع المالي في دول المجلس: القرصنة من خلال طرف ثالث، تخريب بنية أجهزة الصراف الآلي وأنظمة الحاسوب بالمصارف وخروقات مواقع الانترنت والبيانات. كما سنقارن معدلات الاستهداف بالبرمجيات الخبيثة في دول المجلس مع الدول العربية والعالمية الأخرى. وسنقيّم الآثار الاقتصادية والتكاليف المالية التي تنتج عن الهجمات السيبرانية الخبيثة، ونبين مستوى أداء دول المجلس في مواجهة التهديدات الالكترونية ونقارنها مع دول العالم الأخرى والجهود المبذولة لبناء المنعة ضد هذه التهديدات.

والشكل رقم (8) يوضح مدركات وتصوّر المؤسسات (المدراء التنفيذيين) في الشرق الأوسط لأهم التهديدات والمخاطر المثيرة للقلق في المنطقة التي تهدد نموها في الآونة الأخيرة وفقاً لاستطلاع الرأي في عام 2018 الذي اجرته مجموعة PWC البريطانية التي تمثل احدى أكبر الشركات الاستشارية العالمية. ويتبين من الشكل أن التهديدات الإلكترونية تأتي في المرتبة الثانية في قائمة أهم المخاطر المثيرة للقلق لقطاع الشركات في الشرق الأوسط. وارتفع القلق بشأن التهديدات السيبرانية وفقاً لهذا التقرير من نسبة 66 % في عام 2017 إلى نسبة 77 % في عام 2018. والشكل رقم (8) يوضح ترتيب هذه المخاطر والتي تشتمل على: الشكوك أو عدم اليقين الجيوسياسي، التهديدات الالكترونية، التنظيم الزائد عن الحد، الارهاب، سرعة التغير التكنولوجي، زيادة العبء الضريبي، النمو الاقتصادي غير المؤكد والبطالة.

الشكل رقم (8): مدركات وتصوّر الشركات في الشرق الأوسط لأهم التهديدات المثيرة للقلق في عام 2018

المصدر (2018) PWC Report.

أوضاع الأمن السيبراني في الدول العربية وفقاً لدليل الأمن السيبراني العالمي (GCI – Global Cyber security Index)

يقيس دليل الأمن السيبراني العالمي والذي تصدره وحدة الاتصالات العالمية في الأمم المتحدة (ITU) International Telecommunication Unit مستوى التزام الدول المختلفة بالأمن الالكتروني ويوفر المعلومات الاساسية لتحليل ومقارنة أداء الدول العالمية من خلال خمسة ركائز رئيسية وهي العوامل القانونية والفنية والترتيبات التنظيمية وبناء القدرات والتعاون. ويوضح الجدول رقم (7) أوضاع الأمن السيبراني في الدول العربية مقارنة بمناطق العالم الأخرى وفقاً للدليل العالمي للأمن السيبراني. ويتبين من الجدول ان مستوى أداء الدول العربية كان متوسطاً في ركائز أو محاور الدليل الخمسة. وتأتي أوروبا في صدارة المناطق العالمية في الأمن السيبراني، حيث تميزت في كل المحاور وتليها مجموعة الدول المستقلة الروسية بينما تأتي قارة أفريقيا في المرتبة الأخيرة. وقد كان أفضل أداء في الدول العربية من بين هذه المحاور في محور التشريعات القانونية

وأضعفها في المحور التنظيمي. ويوضح الشكل رقم (9) بطاقة الأداء المتوازن للدول العربية في مجال الأمن السيبراني، والتي تعطي تفاصيل أداء الدول في كل محور من المحاور الخمسة المركبة للدليل. وتشير الألوان إلى مستوى المخاطر الالكترونية، فاللون الأحمر يشير إلى ارتفاع مستوى المخاطر والأخضر الى انخفاضها والأصفر الى اعتدالها أو توسطها. ومن الشكل يتضح أن عُمان وقطر ومصر والمغرب هم أقل الدول العربية مخاطراً.

الجدول رقم (7): مستوى أداء الدول العربية في دليل الأمن الالكتروني مقارنة بالمناطق العالمية الأخرى

المنطقة	قانوني	تقني	تنظيمي	تدريبي	تعاوني
أفريقيا	0.29	0.18	0.16	0.17	0.25
الأميركتين	0.40	0.30	0.24	0.28	0.26
الدول العربية	0.44	0.33	0.27	0.34	0.29
آسيا والباسفيك	0.43	0.38	0.31	0.34	0.39
الدول المستقلة الروسية	0.58	0.42	0.37	0.38	0.40
أوربا	0.61	0.60	0.45	0.49	0.46

المصدر: تقرير الأمن السيبراني العالمي 2017.

الشكل رقم (9): بطاقة الأداء المتوازن للدول العربية

Arab States scorecard

المصدر: تقرير الأمن السيبراني العالمي 2017.

أداء دول مجلس التعاون الخليجي في مجال الأمن السيبراني وفقاً للدليل العالمي للأمن السيبراني 2017

احتلت سلطنة عمان المرتبة الأولى عربياً في الدليل العالمي للأمن السيبراني لعام 2017 كما احتلت المركز الأول عربياً في ركيزتي القانون وبناء القدرات في الدليل. وتتمتع سلطنة عُمان بهيكل تنظيمي قوي ووجود إستراتيجية عالية المستوى للأمن السيبراني وخطة رئيسية وخريطة طريق شاملة. واحتلت دولة قطر المرتبة الثانية خليجياً والثالثة عربياً في هذا الدليل لعام 2017 وقد قامت دولة قطر ببناء ثقافة الأمن السيبراني من خلال حملات توعوية مثل حملة يوم الإنترنت الآمن، ونشرت تحذيرات حول التهديدات، مثل الاحتيال والتصيّد عبر الإنترنت، من خلال المطبوعات ووسائل الإعلام الاجتماعية. ويدعم مركز قطر لدراسات الجرائم الإلكترونية ومركز أمن المعلومات الجهود الرامية إلى حماية الجمهور القطري ومكافحة المجرمين الذين يستخدمون التكنولوجيا لتنفيذ أنشطتهم الخبيثة.

والجدول رقم (8) يوضح الأوضاع العامة للمخاطر الالكترونية في دول مجلس التعاون الخليجي. ويشير الدليل الكلي للأمن السيبراني الى انخفاض المخاطر الالكترونية في كل من عُمان وقطر وارتفاعها في الكويت وتوسطها في السعودية والإمارات. وعلى مستوى المؤشرات الفرعية للدليل العام، يدل الجدول على أن مخاطر التشريعات السيبرانية في دول المجلس تتراوح بين المتوسطة إلى المنخفضة، مما يبيّن أن بعض الدول تحتاج إلى تقوية التشريعات السيبرانية لسد الثغرات في القانون التي يمكن أن يستغلها مجرمو الانترنت.

ويحتوي المؤشر العام للإجراءات القانونية على مؤشرات فرعية تقيس مخاطر التشريعات الأمنية السيبرانية وتشريعات الجريمة السيبرانية والتدريب في مجال الأمن السيبراني ويتراوح مستوى المخاطر الذي تواجهه دول المجلس في هذه المؤشرات الفرعية بين المتوسط والمنخفض باستثناء الكويت التي تشير البيانات إلى وجود مخاطر عالية في معظم المؤشرات القانونية.

أما المؤشر العام للإجراءات التقنية في دول المجلس، فيشير الى انخفاض المخاطر السيبرانية في هذا المجال في عُمان وقطر والسعودية وتوسطها في البحرين والإمارات وارتفاعها في

الكويت. بينما يشير المؤشر العام للإجراءات التنظيمية الى انخفاض المخاطر السيبرانية في هذا المحور في عمان وقطر وتوسطها في البحرين والامارات وارتفاعها في السعودية والكويت. ويحتوي المؤشر العام للإجراءات التنظيمية على عدة مؤشرات فرعية هي وجود الاستراتيجية السيبرانية والهيئة المسئولة ووجود مقاييس للأمن السيبراني في الدولة. وتشير هذه المؤشرات الفرعية إلى ارتفاع المخاطر في مؤشرات الاستراتيجية ومقاييس الأمن السيبراني في معظم دول المجلس.

ويشير المؤشر العام لبناء القدرات إلى انخفاض المخاطر السيبرانية في عُمان وقطر والسعودية وتوسطها في الامارات وارتفاعها في الكويت والبحرين. ويحتوي هذا المؤشر على مؤشرات فرعية تتمثل في وجود هيئات وضع المعايير وأفضل الممارسات في الأمن السيبراني وبرامج البحث والتطوير والحملات التوعوية العامة والبرامج التعليمية وآلية الحوافز والصناعات المحلية.

وفقاً للمؤشر العام للتعاون، فإن دول المجلس تواجه عموماً مخاطر متوسطة في هذا المجال. ويتركب هذا المؤشر العام من مؤشرات فرعية هي: الاتفاقات الثنائية والاتفاقات متعددة الأطراف والمشاركة الدولية وشراكة القطاع العام والخاص والشركات التكاملية. وترتفع المخاطر من بين هذه المؤشرات الفرعية في دول المجلس في مؤشرات الشراكة بين القطاع العام والخاص والشراكات التكاملية مما يدل على أهمية تعزيز الجهود المبذولة في هذه الجوانب.

الجدول رقم (8): أوضاع الأمن السيبراني في دول مجلس التعاون الخليجي وفقاً للدليل العالمي للأمن السيبراني (2017)

الدولة	المؤشر العام للإجراءات القانونية	المؤشر العام للإجراءات التقنية	المؤشر العام للإجراءات التنظيمية	المؤشر العام لبناء القدرات	المؤشر العام للتعاون	الدليل العام للأمن السيبراني GCI 2017
البحرين	منخفض	متوسط	متوسط	عالي	متوسط	متوسط
الكويت	عالي	عالي	عالي	عالي	عالي	عالي
عُمان	منخفض	منخفض	منخفض	منخفض	منخفض	منخفض
قطر	منخفض	منخفض	منخفض	منخفض	متوسط	منخفض
السعودية	متوسط	منخفض	عالي	منخفض	متوسط	متوسط
الإمارات	منخفض	متوسط	متوسط	متوسط	متوسط	متوسط

المصدر: تقرير الأمن السيبراني العالمي 2017 – الأمم المتحدة.

جهود دول مجلس التعاون الخليجي في تعزيز الأمن الالكتروني

بذلت حكومات دول مجلس التعاون الخليجي جهود كبيرة في تعزيز الأمن السيبراني فعلى سبيل المثال: قامت حكومة دبي بنشر خطتها الاستراتيجية للأمن السيبراني وخطة الإمارات للحواجز المتسلسلة (Block Chain)، كما أنشأت السعودية الهيئة القومية للأمن السيبراني في عام 2017. واتخذت بعض البلدان العربية مثل البحرين وعُمان والإمارات والسعودية والمغرب عدة خطوات لسن قوانين تتعلق بالجرائم الالكترونية وأنشأت أنظمة خاصة بذلك. وتهدف بعض هذه القوانين (كما في حالة الإمارات وعُمان والمغرب) إلى حماية المعاملات الالكترونية وملاحقة مجرمي الانترنت ولكنها تعاني من العديد من الثغرات. ولاتزال التشريعات السيبرانية في المنطقة العربية عموماً إما في مرحلة أولية أو قيد التطوير النشط.

كما قامت دول المجلس بوضع استراتيجيات للأمن السيبراني بهدف تخطيط وتنفيذ وإدارة ومتابعة البرامج والمشاريع التي تعزز هذا الجانب. فقامت دولة الكويت، على سبيل المثال، بوضع الاستراتيجية الوطنية للأمن السيبراني للفترة 2017-2020. وتتمثّل رؤية الاستراتيجية في "ضمان فضاء الكتروني آمن ومرن لحماية المصالح الوطنية لدولة الكويت" من المخاطر والتهديدات السيبرانية وتحقيق أكبر قيمة اقتصادية واجتماعية من استخدام الفضاء الالكتروني. وتتمحوّر مهمة الاستراتيجية حول "خلق وتعزيز منظومة الأمن السيبراني الوطني بجميع عناصرها التقنية والتنظيمية والرقابية والادارية وفي مختلف الجهات الحكومية والقطاع الخاص وتوفير بيئة فضاء الكتروني آمنة لتعزيز الأمن والازدهار لجميع الذين يعيشون ويعملون في دولة الكويت". وتسعى الاستراتيجية الى تحقيق ثلاثة أهداف رئيسية على النحو التالي:

أولاً: تعزيز ثقافة الأمن السيبراني التي تدعم الاستخدام الآمن والصحيح للفضاء الالكتروني.

ثانيا: حماية ومراقبة الأصول والبنى التحتية الحيوية والمعلومات الوطنية والشبكة المعلوماتية في دولة الكويت.

ثالثاً: اتاحة سبل التعاون والتنسيق وتبادل المعلومات فيما بين مختلف الجهات المحلية والدولية في مجال الأمن السيبراني.

وتقوم البنوك المركزية في دول مجلس التعاون الخليجي كجهات تنظيمية ورقابية للقطاعات المالية ببذل جهود كبيرة لضمان الاستقرار المالي الكلي ومواجهة التهديدات السيبرانية وتخفيف آثارها الاقتصادية والمالية. ونورد على سبيل المثال جهود بنك الكويت المركزي في تعزيز الأمن السيبراني في دولة الكويت كنموذج لجهود البنوك المركزية في دول المجلس وفقاً لتقريره السنوي للعام (2018/2017). وتضمنت هذه الجهود اصدار تعليماته للبنوك المحلية بموجب الكتاب الموجه لاتحاد مصارف الكويت بتاريخ 26 / 11 / 2017 بشأن الحد الأدنى من المعايير المطلوبة لمواجهة سرقة بيانات أجهزة الصرف الآلي ومكافحة عمليات الغش باستخدام هذه الأجهزة. ورفع البنك لمستوى الحماية والضوابط الأمنية على شبكته الداخلية عن طريق تطبيق نظام التحكم في الوصول الى الشبكة المحلية السلكية واللاسلكية، بالإضافة الى تطبيق خدمة الكشف عن الثغرات ونقاط الضعف بشبكة بنك الكويت المركزي الخاصة بنظام مايكروسوفت التشغيلي وذلك بالتنسيق مع مختصين بالأمن السيبراني من شركة مايكروسوفت العالمية. وقد أشادت الشركة بجهود بنك الكويت المركزي في اتباع وتطبيق آخر التحديثات والضوابط الأمنية الصادرة منها والحفاظ على بيئة آمنة للبنك. بالإضافة الى الانتهاء من تطبيق مشروع خدمة حماية السمعة للبنك المركزي ورصد ومراقبة كل ما يهددها من المخاطر الالكترونية واتخاذ الخطوات اللازمة لمعالجتها فوراً.

كما قام البنك بتقييم المخاطر في إدارة نظم المعلومات والانتهاء من اختبارات الاختراق لأنظمة البنك بهدف كشف الثغرات وتقييم المستوى الأمني لها بالإضافة إلى التأكد من سلامة نظم المعلومات واتباع أفضل وأحدث الممارسات العالمية في مجال أمن المعلومات. وإعداد برنامج تدريبي في مجال أمن المعلومات لتأهيل الكوادر الوطنية في القطاع المصرفي لمواجهة التحديات الأمنية المتزايدة والمتسارعة التي تواجه هذا القطاع بدولة الكويت (التقرير السنوي لبنك الكويت المركزي، 2017).

سابعاً: نماذج للهجمات الالكترونية على القطاعات الاقتصادية الحيوية في دول مجلس التعاون الخليجي

نستعرض في هذا الجزء من الدراسة نماذج للهجمات الالكترونية على القطاع المالي والنفطي في دول مجلس التعاون الخليجي بهدف توضيح إمكانية حدوث اختراقات واسعة النطاق على قطاعات حيوية وإمكانية الحاق الضرر بملايين الأفراد وتكرار الهجوم من نفس البرمجيات الخبيثة المستخدمة سابقاً والنجاح في الحاق الضرر مرة أخرى.

1. نماذج من الهجمات السيبرانية على القطاع المالي في دول مجلس التعاون الخليجي

بالتزامن مع الاتجاهات العالمية السائدة اليوم، استمر حجم التهديدات السيبرانية في الارتفاع عدداً وتنوعاً في دول مجلس التعاون الخليجي. وتعتبر المخاطر والهجمات السيبرانية وخروق خصوصية المعلومات من أكبر التحديات التي تواجه القطاع المالي في دول المجلس، فمع زيادة الخدمات المالية عبر الهاتف المحمول والاستعانة بمصادر خارجية (outsourcing) في تقديمها تزداد مخاطر حماية المستهلك وتنظيم القطاع المالي غير المصرفي. وتُمثل الهجمات السيبرانية أعظم المخاطر التي تواجه هذا القطاع وذلك بسبب ازدياد تواترها وعدم إمكانية التنبؤ بها وتأثيرها القطاعي المحتمل ووجود الثغرات في إدارة مخاطرها (صندوق النقد الدولي، 2018). وتضمنت أصناف الهجمات على القطاع المالي في دول المجلس: القرصنة من خلال طرف ثالث وتخريب بنية أجهزة الصراف الآلي وأنظمة الحاسوب بالمصارف وخروقات مواقع الانترنت والبيانات، على النحو التالي:

أ. القرصنة عبر طرف ثالث

تمكن مجرمو الانترنت من اختراق مركزين لمعاجلة البطاقات الالكترونية في الهند والتي تتولى مهمة عمليات الدفع لبطاقات الدفع المسبق لمصرفين أحدهما في عُمان والآخر بالإمارات العربية المتحدة. وقد قام المجرمون بزيادة الأرصدة المتاحة وسقوف السحب على البطاقات الائتمانية مسبقة الدفع بالإضافة إلى إدخال بطاقات مُرمّزة زائفة والتي مكّنتهم من سحب 45 مليون دولار من أجهزة الصراف الآلي في 27 دولة.

ب. تخريب البنية التحتية لأجهزة الصراف الآلي

استخدم مجرمو الانترنت في عام 2016 برمجيات خبيثة خاصة تُجبر أجهزة الصراف الآلي على صرف النقود في عدد من دول الشرق الأوسط. وقد كانت الإمارات العربية هدفاً لعدد من هذه الهجمات. فقد استهدفت هذه الهجمات مركز بيانات أجهزة الصرف الآلي والتي مكّنت المجرمون من التقاط البيانات الخاصة بالعملاء بما في ذلك رقم حساب العميل المصرفي والرقم السري للبطاقة للائتمانية (PIN) المستخدم في الصرف الآلي بالإضافة إلى السرقة المباشرة للنقود.

ج. اختراق أنظمة الحاسوب بالبنوك

قام مجرمو الانترنت باختراق أنظمة الحاسوب بالبنوك الخليجية باستخدام رسائل البريد الالكتروني الخبيثة وبرامج القرصنة مما نتج عنها خسائر كبيرة في بعض الدول في عام 2017.

د. الحرمان من الخدمة الموزّعة

اخترق مجرمو الانترنت في عام 2012 المواقع الالكترونية في العديد من المؤسسات المالية العربية والتي شملت بورصة أبوظبي للأوراق المالية، والبورصة السعودية، ومواقع البنك المركزي في الإمارات والبنك العربي الفلسطيني.

هـ. خروقات البيانات Data Breaches

تمكّن مجرمو الانترنت من القرصنة على أحد البنوك الإماراتية وطالبوا بدفع الفدية بالعملة الرقمية (Bit Coin) في مقابل عدم تسريب المعاملات المالية السرية وتفاصيل العميل على الشبكات الاجتماعية في عام 2015. كما عانى أحد أكبر بنوك قطر من اختراق للبيانات الخاصة والذي تضمّن بيانات العملاء الخاصة في عام 2016 (Lukonga، 2018).

2. نماذج من الهجمات السيبرانية على القطاع النفطي في دول مجلس التعاون الخليجي استهداف شركة أرامكو السعودية عام 2012

شهدت الشركة السعودية للبترول «أرامكو» واحدة من أسوأ عمليات القرصنة التي حدثت في دول المجلس في يوم 2012/8/15 حيث تم الهجوم على شبكة الحاسوب في الشركة بفيروس يستنسخ نفسه ذاتياً مما تسبب في تدمير أو مسح بيانات أكثر من 30 ألف حاسب آلي، وأصبحت الشركة غير قادرة على الوفاء بالتزاماتها تجاه الآخرين وغير قادرة على تلقي بيانات المعاملات النقدية عبر أجهزة الحاسب أو استخراجها، وعلى الرغم من ضخامة موارد الشركة الا انها استغرقت حوالي أسبوعين للتعافي من تلك الاضرار مما أدى الى خسائر مالية فادحة. وقد تمثّلت مهمة الفيروس الخبيث الذي يسمى شمعون (Shamoon) في مسح البيانات في الأقراص الصلبة في أجهزة

الحاسوب. وقد نجح هذا الهجوم في الحاق الضرر بقطاع النفط رغم الاحتراز الكبير والحرص من الحكومة السعودية والأمريكية على استمرارية تدفق النفط عالمياً وعلى استقرار أسعاره.

نموذج تكرار الهجوم من نفس البرمجيات الخبيثة المستخدمة سابقاً: فيروس شمعون الخبيث يهاجم مرة أخرى:

تعرضت أفرع الشركة الإيطالية Saipem التي تعمل في قطاع الطاقة في الشرق الأوسط وابردين في بريطانيا وإيطاليا لهجوم فيروس يعمل على مسح بيانات الأنظمة الحاسوبية (فيروس شمعون) في عام 2018، وقد استخدم هذه البرمجية الخبيثة في مهاجمة شركة أرامكو السعودية عام 2012. وعلى الرغم من عدم حدوث اضراراً باهظة للشركة الا أن هذه الحوادث تؤكد ارتفاع مخاطر تكرار الهجوم من نفس البرمجيات الخبيثة المستخدمة سابقاً. وبالمثل، عانت شركة هندسية إماراتية أخرى من نفس الفيروس في 2018/12/10 قبل يوم واحد من الهجوم على الشركة الإيطالية، وقد حذر مركز دبي للأمن الالكتروني (DESC) من هذا الهجوم.

بالإضافة الى النماذج السابقة تبرز نماذج أخرى للهجمات السيبرانية في دول المجلس ذات أهمية كبيرة لما لها من تأثير على كبير على الافراد والمجتمع نذكر منها على سبيل المثال نموذج افشاء البيانات الشخصية في شركة كريم لخدمات نقل الركاب في دبي وهي شركة للأجرة الخاصة في الشرق الأوسط وتعد المنافس الأول لشركة أوبر في المنطقة، وتأسست في عام 2012. وتعرضت هذه الشركة لهجوم الكتروني خبيث حيث تمكّن من خلاله المهاجمون من الدخول على قواعد بيانات الموظفين والزبائن. وتأثرت بهذا الهجوم البيانات الشخصية لحوالي 14 مليون شخص، وتضم هذه البيانات المسروقة أسماء الأشخاص وأرقام هواتفهم وبريدهم الالكتروني. ويتجلى من هذه التجربة إمكانية الحاق الضرر بملايين الأفراد في هجوم سيبراني واحد وأن الشركات في دول مجلس التعاون الخليجي بمختلف أحجامها قد تكون معرضة للهجوم الخبيث الذي يؤدي الى فقدان الثقة في الشركة والخسائر المالية الكبير والميزة التنافسية في الأسواق.

ثامناً : تحليل الآثار الاقتصادية للهجمات الالكترونية في دول مجلس التعاون الخليجي

كانت أعلى القطاعات استهدافاً في دول مجلس التعاون الخليجي في عام 2015 هي القطاعات الحكومية وقطاع الطاقة وقطاع الخدمات المالية وشكّلت هذه القطاعات الثلاثة وحدها نسبة 65% من الهجمات التي تم تحديدها في ذلك العام. ويرجع سبب ذلك الى المكانة التي تتمتع بها دول مجلس التعاون الخليجي كمركز للتمويل والطاقة والخدمات العامة والسياحة والطيران مما جعلتها في مقدمة الوجهات العالمية المستهدفة بشكل واسع من قبل مجرمي الإنترنت، وساعد على ذلك تطور البنيات التحتية للمعلوماتية والاتصالات في المنطقة والتي جعلت منها بيئة خصبة للهجمات الإلكترونية المعقّدة. وقد تعرضت الشركات في الشرق الأوسط لخسائر مالية في عام2016 أكبر من غيرها من المناطق العالمية الأخرى بسبب للحوادث السيبرانية، حيث عانت نسبة 56% من الشركات التي تم استهدافها في المنطقة من خسائر مالية فاقت نصف مليون دولار وذلك مقارنة بنسبة 33 % على الصعيد العالمي، كما خسرت نسبة 13% منها ما لا يقل عن ثلاثة أيام عمل وذلك مقارنة بنسبة 9 % على المستوى العالمي كما هو موضح في الجدول رقم (9)، كما أن احتمالية التعرض والمعاناة من هذه الهجمات في شركات الأعمال في الشرق الأوسط أعلى من غيرها من بقية مناطق العالم الأخرى، فشهدت نسبة 18 % من المؤسسات في المنطقة أكثر من 5000 هجوم ، وهو أعلى من أي منطقة أخرى في العالم، مقارنة بمتوسط عالمي يبلغ 9% فقط (PWC Report 2016).

الجدول رقم (9): خسائر الشركات في الشرق الأوسط من الهجمات السيبرانية الخبيثة مقارنة بالمناطق العالمية الأخرى (2016)

أنواع الخسائر التي عانت منها الشركات	الشرق الأوسط (٪)	العالم (٪)
خسائر مالية تتجاوز مبلغ 50000 ألف دولار	56	33
أضرار بالسمعة التجارية	16	22
توقف الأعمال التجارية لمدة ثلاثة أيام أو أكثر	13	9
حوادث سيبرانية يتراوح عددها بين 5000-99,999 حادث	13	6

المصدر: PWC Report 2016

يوضح الجدول السابق أن الشركات في الشرق الأوسط تعاني من خسائر مالية بسبب الهجمات السيبرانية أعلى من غيرها من الشركات المثيلة في مناطق العالم الأخرى، حيث تجاوزت هذه الخسائر مبلغ 500 ألف دولار في أكثر من نصف شركات المنطقة مقارنة بثلث الشركات العالمية المثيلة في المناطق الأخرى، كما عانت نسبة 13 % من الشركات العاملة في المنطقة من فقدان ثلاثة أيام عمل مقارنة بنسبة 9 % في الشركات العالمية الأخرى.

وقد تمثلت الهجمات السيبرانية في المنطقة في سرقة البيانات والاحتيال الالكتروني والتصيّد وغيرها من الأنواع الأخرى. وترجع أسباب ارتفاع اعداد الهجمات السيبرانية في المنطقة مقارنة بالمناطق الأخرى إلى عِظَم انتشار البرمجيات الخبيثة في المنطقة أكثر من غيرها من المناطق الأخرى، وارتفاع عمليات الاحتيال عبر الفاكس بشكل أعلى من المعتاد عليه عالمياً والتي يصعُب تتبعها من خلال النظام المركزي للشركات (PWC Report 2016).

وأشارت دراسة CSIS & McAfee في عام (2018) إلى أن دولة الإمارات العربية تحتل المرتبة الثانية عالمياً في قائمة الدول المستهدفة بالهجمات السيبرانية بما يُقدّر تكلفته بحوالي 1.4 مليار دولار في العام. وينتج عن زيادة معدلات نمو الهجمات السيبرانية اهتزاز الثقة في الاقتصاد الرقمي الذي تسعى دول المجلس أن تطوره من خلال الشروع في تطوير المدن الذكية (Smart-Cities) في عدد من هذه البلدان.

تصدّرت دول المجلس القائمة العالمية في الاستهداف في بعض أنواع الهجمات السيبرانية الخبيثة، فاحتلت عُمان المرتبة الرابعة في مجال معدلات البرمجيات الخبيثة بالبريد الالكتروني تلتها السعودية في المرتبة الخامسة والكويت في المرتبة الثامنة كما هو موضح في الجدول رقم (10-A)، واحتلت السعودية المرتبة الأولى عالمياً في مجال البريد الالكتروني المؤذي وجاءت الكويت في المرتبة السادسة والإمارات في المرتبة العاشرة في هذه القائمة كما هو موضح في الجدول رقم (10-B) وفقاً لتقرير (ISTR) في عام (2018). وتدل هذه الجداول على ارتفاع بعض أنواع الهجمات السيبرانية في دول مجلس التعاون الخليجي مقارنة بالمناطق العالمية الأخرى. وعموماً، تتعرض دول المجلس لكل أنواع الهجمات الإلكترونية الضارة ولكن بنسب متفاوتة مما يؤكد على عظم مخاطر التهديديات الالكترونية.

الجدول رقم (10-A): معدلات البرمجيات الخبيثة بالبريد الالكتروني حسب الدولة

الترتيب	الدولة	برمجية واحدة في كل ايميل
1	النمسا	102
2	المجر	108
3	أندونيسيا	140
4	عمان	156
5	السعودية	175
6	جزر الأنتيل الهولندية	184
7	ماليزيا	216
8	الكويت	217
9	جنوب أفريقيا	233
10	تايوان	234

المصدر: (2018) ISTR Report.

الجدول رقم (10-B): معدلات البريد الالكتروني المؤذي حسب الدولة (Spam)

الترتيب	الدولة	النسبة
1	السعودية	69.9
2	الصين	68.6
3	البرازيل	64.7
4	سريلانكا	64.6
5	المجر	60.4
6	الكويت	59.8
7	عمان	58.9
8	جنوب أفريقيا	57.1
9	النرويج	56.9
10	الإمارات	56.3

المصدر: (2018) ISTR Report.

مقارنات دولية في التكاليف الاقتصادية والمالية للهجمات الالكترونية: نموذج دولة الامارات العربية المتحدة

ونستعرض الآثار الاقتصادية للهجمات الالكترونية في دولة الامارات العربية المتحدة كنموذج توضيحي وفقاً لاستطلاع الرأي الذي قامت به شركة نورتون العالمية في عام 2017. والجدول رقم (11) يبيّن الآثار الاقتصادية للهجمات الالكترونية على الاقتصاد الاماراتي. ويدُل الجدول على ارتفاع التكاليف الاقتصادية والمالية للهجمات الالكترونية في دولة الامارات مقارنة بدول العالم الأخرى مما يجعلها واحدة من أعلى الدول العالمية المستهدفة بهذه الهجمات. فبلغ إجمالي المستهلكين المتضررين من الجريمة السيبرانية في عام 2017 في الامارات 3.72 مليون شخص من جملة السكان وتجاوزت التكلفة المالية الإجمالية للجريمة السيبرانية مليار دولار، بينما ارتفع الوقت الإجمالي الذي خسره المستهلك بسبب هذا النوع من الجرائم 47.9 ساعة مقارنة بمتوسط عالمي بلغ 23.6 ساعة أي بما يعادل الضعف. كما فاقت نسبة المستهلكين المتأثرين بجرائم الإنترنت في الامارات المتوسط العالمي فبلغت 52% مقارنة بمتوسط عالمي بلغ 44 %.

وقد كان أكثر أنواع الجرائم السيبرانية شيوعاً في الامارات في 2017 هي عدوى البرمجيات الخبيثة وهي بذلك مطابقة لمثيلاتها في العالم. ولكن تجاوزت نسبة العدوى فيها المتوسط العالمي فبلغت نسبة 53 % مقارنة بمتوسط عالمي هو 48 %. وبلغت النسبة المئوية لضحايا الجرائم الإلكترونية الذين يشاركون كلمة المرور الخاصة بحساب واحد على الأقل عبر الإنترنت مع آخرين نسبة 45 % في الامارات مقارنة بمتوسط عالمي هو 42 %. بينما بلغت نسبة ضحايا الجرائم الإلكترونية الذين يستخدمون نفس كلمة المرور عبر جميع الحسابات عبر الإنترنت 24 % في الامارات مقارنة بنسبة 20 % في العالم. وتقاربت النسبة المئوية لضحايا برمجيات الفدية الخبيثة الذين دفعوا الفدية ولم يتمكنوا من الوصول إلى ملفاتهم في كل من الامارات ودول العالم الأخرى فبلغت هذه النسبة 18 % في الامارات و17 % في المتوسط العالمي. وقد كانت أكثر حوادث الجريمة السيبرانية تكلفة بالنسبة للمستهلكين في العام الماضي في الامارات هي الاحتيال على البطاقات الائتمانية بما يعادل 1051 دولار بينما كانت الجريمة الأكثر تكلفة عالمياً هي سرقة الهوية بمتوسط 838 دولار.

الجدول رقم (11): الآثار الاقتصادية للهجمات الالكترونية الخبيثة على الاقتصاد الاماراتي (2017)

النتائج	دولة الامارات	العالم
إجمالي المستهلكين المتضررين من الجريمة السيبرانية في العام الماضي	3.72 مليون	978 مليون
التكلفة المالية الإجمالية للجريمة السيبرانية في العام الماضي	1.05 مليار دولار	172 مليار دولار
الوقت الإجمالي لكل مستهلك خسره بسبب الجريمة السيبرانية في العام الماضي	47.9 ساعة	23.6 ساعة
نسبة المستهلكين المتأثرين بجرائم الإنترنت في العام الماضي	%52	%44
أكثر أنواع الجرائم السيبرانية شيوعاً في العام الماضي	عدوى البرمجيات الخبيثة %53	عدوى البرمجيات الخبيثة %48
النسبة المئوية لضحايا الجرائم الإلكترونية الذين يشاركون كلمة المرور الخاصة بحساب واحد على الأقل عبر الإنترنت مع آخرين مقابل غير الضحايا	%45 %20	%42 %23
ضحايا الجرائم الإلكترونية الذين يستخدمون نفس كلمة المرور عبر جميع الحسابات عبر الإنترنت مقابل غير الضحايا	%24 % 20	%20 %16
النسبة المئوية لضحايا برمجيات الفدية الخبيثة الذين دفعوا الفدية ولم يتمكنوا من الوصول إلى ملفاتهم	%18	%17
أكثر حوادث الجريمة السيبرانية تكلفة بالنسبة للمستهلكين في العام الماضي	الاحتيال على البطاقات الائتمانية (بقيمة 1051 دولار)	سرقة الهوية (بقيمة 838 دولار)

المصدر: Symantec Corporation - Norton cyber security – insight report 2017

تاسعاً: الخاتمة والتوصيات

ان ازدياد ابتكارات التكنولوجيا الرقمية الحديثة في الآونة الأخيرة مثل انترنت الأشياء (Internet of Things) والحواجز المتسلسلة Block Chain وخدمات الحوسبة السحابية (Cloud services) قد زادت من ترابط دول العالم والأفراد والشركات وستتضاعف اعداد أجهزة الحاسوب المرتبطة مع بعضها البعض إلى أكثر من ثلاثة أضعاف خلال الفترة 2015-2020، كل هذه المعطيات جعلت المنظمات الدولية مثل صندوق النقد الدولي (IMF) والمنتدى الاقتصادي العالمي (WFE) تضع المخاطر الالكترونية في صدارة المخاطر التي تواجه النظام الاقتصادي العالمي وتدعو لبناء المنعة ضد هذه المخاطر بسبب عِظَم آثارها الاقتصادية.

وحاولت هذه الدراسة تسليط الضوء على أهمية هذه المخاطر وآثارها الاقتصادية وكيفية إدارتها، وأعطت نماذج دولية لحوادث الإصابة بها. ثم حلّلت وقيّمت أوضاع دول مجلس التعاون الخليجي كنموذج أو دراسة حالة. وهدفت الى زيادة الاهتمام بالاستثمار واستدراك الثغرات في التخطيط الاقتصادي لمجابهة هذه المخاطر.

ويواجه صانعو القرار في الدول في الدول العربية عموماً تحديات عظيمة في المحافظة على الاستقرار المالي والاقتصادي في ضوء تنامي المخاطر الالكترونية وتنوعها وتفاوت أسبابها وبروزها كمخاطر نظامية تهدد الأنشطة الاقتصادية الحيوية والقطاع المالي. وتأتي قطاعات الخدمات المالية والنفط في قائمة القطاعات المستهدفة عالمياً بالهجمات السيبرانية. وتتصدر دول مجلس التعاون الخليجي دول العالم الأخرى في بعض أنواع الهجمات السيبرانية على الأنشطة الاقتصادية مثل معدلات البرمجيات الخبيثة بالبريد الالكتروني ونسب البريد الالكتروني المؤذي (Spam). كما تفوق الخسائر الناجمة عن الهجمات الالكترونية في دول المجلس المتوسط العالمي ولا يمكن استرداد معظم الخسائر المالية الناجمة عنها. وأثبتت نماذج الهجمات الالكترونية السابقة على دول المجلس إمكانية إلحاق الضرر بالمرافق الحيوية والبنيات التحتية بهذه الدول مما يحتم بذل المزيد من الجهود لسد الثغرات في الأمن الالكتروني بهذه الدول.

وعلى الرغم من تحسن أداء دول المجلس في مجال مواجهة الهجمات الالكترونية، إلا أن الدليل العالمي للأمن السيبراني الذي تصدره الأمم المتحدة يشير إلى وجود العديد من الثغرات القانونية والفنية والتنظيمية والتدريبية والتعاونية التي يجب سدها من خلال تحسين الأداء والإكمال والمراجعة للوضع الراهن في هذه الجوانب وذلك من خلال زيادة الاستثمار في التدريب وبناء القدرات ضد هذه الهجمات بالإضافة إلى رفع الوعي بين المستخدمين والإدارة العليا بأهمية وكيفية التعامل مع هذه الهجمات، وتعزيز التعاون الدولي لمواجهة المخاطر الالكترونية وذلك لطبيعة هذه المخاطر ولأن مجابهتها قد تكون أكبر من قدرات الدولة الواحدة أو خارج سيطرتها. وعلى مستوى المؤسسات، يجب إدراج الأمن السيبراني ضمن استراتيجية إدارة المخاطر في المؤسسة.

وعلى الرغم من ارتفاع الإنفاق في الأمن السيبراني في دول مجلس التعاون الخليجي في الآونة الأخيرة الا أنه لا يكفي بمفرده في مواجهة التهديدات وتحقيق الأمن السيبراني في دول المجلس

بل لابد من تحسين الوعي والحوكمة والعمليات (أو المعالجات) لأن هذه المنطقة هي إحدى أكثر مناطق العالم تقدماً في سرعة تبني واعتماد التكنولوجيا الحديثة.

المراجع الانجليزية

Bank of England, (2017), "Systemic Risk Survey Results – 2017 H2", November, London.

Bouveret, A. (2018), "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment", IMF Working paper (WP/18/143).

Central bank of Kuwait, (2018), "Annual Report 2017/2018" in Arabic. http://www.cbk.gov.kw/en/statistics-and-publication/publications/annual-reports.jsp.

Center for Strategic and International Studies (CSIS) and McAfee, (2018), "Economic Impact of Cybercrime— No Slowing Down" February. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact- cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email.

Council of Economic Advisors (CEA) - The Whitehouse - USA. (2018), "The Cost of Malicious Cyber Activity to the U.S. Economy", https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

Depository Trust & Clearing Corporation (DTCC), (2017)., "Systematic Risk Barometer: Results Overview – 2017 Q1", http://www.dtcc.com/news/2017/may/22/dtcc-systemic-risk-barometer-survey-reveals-increased-concerns-over-cyber-risk.

International Communication Unit, (2017), "Global Cybersecurity Index (GCI) 2017", July.

Kopp, E., L. Kaffenberger, and C. Wilson. (2018), "Cyber Risk, Market Failures, and Financial Stability", IMF Working Paper (WP/17/185).

Lukonga, I. (2018). " Fintech, Inclusive Growth and Cyber Risks: A Focus on the MENAP and CCA Regions", IMF Working Paper, WP/18/201, https://www.imf.org/en/Publications/WP/Issues/2018/09/11/Fintech-Inclusive-Growth-and-Cyber-Risks-Focus-on-the-MENAP-and-CCA-Regions-46190.

McAfee, Inc. (2014). Net Losses: Estimating the Global Cost of Cybercrime. Center for Strategic and International Studies, June. Santa Clara, CA: McAfee, http://www. mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Ponemon Institute, (2017), "2017 Cost of Data Breach Study", June.

Ponemon Institute LLC and Accenture (2017). "Cost of Cyber Crime Study-2017", https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

PWC - Global State of Information Security® Survey. (2016), "A false sense of security? Cybersecurity in the Middle East", March. https://www.pwc.com/m1/en/publications/documents/middle-east-cyber-security-survey.pdf.

PWC - pwc-22nd-annual-global-ceo-survey. https://www.pwc.com/gx/en/ceo-survey/2019/report/pwc-22nd-annual-global-ceo-survey.pdf.

State of Kuwait- citra, (2017), ""National Cyber Security Strategy of the State of Kuwait 2017-2020", https://citra.gov.kw/sites/en/LegalReferences/English%20Cyber%20Security%20Strategy.pdf

Symantec Corporation – US . (2017)., " 2017 Norton Cyber Security Insights Report: Global Comparisons", https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-comparison-uae-en.pdf

Symantec Corporation. (2018), “ISTR - Internet Security Threat Report”, vol. 23. https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

United Nation - International Telecommunication Union (ITU), the World Bank, Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organization (CTO), and NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE). (2018)., “Guide to Developing a National Cybersecurity Strategy”, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

World Economic Forum, (2012). “Partnering for Cyber Resilience”, http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf.

World Economic Forum, (2015)., “Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats” January 2015, available at http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf.

World Economic Forum, The Boston Consulting Group and Hewlett Packard Enterprise. (2017). “Advancing Cyber Resilience Principles and Tools for Boards”, http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf.

World Economic Forum, (2018), “The Global Risks Report 2018: Insight Report, 13th Edition”, http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

صدر عن هذه السلسلة :

1 - مواءمة السياسات المالية والنقدية بدولة الكويت لظروف ما بعد التحرير
د. يوسف الابراهيم ، د. أحمد الكواز

2 - الأوضاع والسياسات السكانية في الكويت بعد تحريرها
د. ابراهيم العيسوي (محرر)

3 - إعادة التعمير والتنمية في الكويت
د. عمرو محي الدين

4 - بعض قضايا الإصلاح الاقتصادي في الأقطار العربية
د. جميل طاهر ، د. رياض دهال ، د. عمادالامام

5 - إدارة الموارد البشرية وتخطيط التعليم والعمالة في الوطن العربي
د. محمد عدنان وديع

6 - حول مستقبل التخطيط في الأقطار العربية
د. ابراهيم العيسوي

7 - مشاكل التعليم وأثرها على سوق العمل
د. محمد عدنان وديع

8 - أهداف التنمية الدولية وصياغة السياسات الإقتصادية في الدول العربية
د. علي عبد القادر علي

9 - تحديات النمو في الاقتصاد العربي الحديث
د. عماد الإمام

10 - هل تؤثر السياسات الاقتصادية الكلية على معدلات نمو الدول العربية؟
د. علي عبد القادر علي

11 - الصيرفة الإسلامية : الفرص والتحديات
د. محمد أنس الزرقا

12 - دور التجارة العربية البينية في تخفيف وطأة النظام الجديد للتجارة
اعداد : د. محمد عدنان وديع ، تحرير : أ. حسان خضر

13 - العولمة وقضايا المساواة في توزيع الدخل في الدول العربية
اعداد : د. علي عبد القادر علي

علم الدين بانقا

14 - السياسات الكلية وإشكالات النمو في الدول العربية
اعداد : أ. عامر التميمي ، تحرير : د. مصطفى بابكر

15 - الجودة الشاملة وتنافسية المشروعات
اعداد : أ.د. ماجد خشبة ، تحرير : د. عدنان وديع

16 - تقييم أدوات السياسة النقدية غير المباشرة في الدول العربية
إعداد: د. عماد موسى، تحرير : د. أحمد طلفاح

17 - الأضرار البيئية والمحاسبة القومية المعدلة بيئيا : إشارة لحالة العراق
إعداد: د . أحمد الكواز

18 - نظم الإنتاج والإنتاجية في الصناعة
إعداد: م . جاسم عبد العزيز العمّار، تحرير: د. مصطفى بابكر

19 - اتجاهات توزيع الإنفاق في الدول العربية
إعداد: د . علي عبدالقادر علي، تحرير: د. رياض بن جليلي

20 - هل أضاعت البلدان العربية فرص التنمية؟
إعداد: د . أحمد الكواز

21 - مأزق التنمية بين السياسات الاقتصادية والعوامل الخارجية
إعداد: د . أحمد الكواز

22 - التنمية وتمكين المرأة في الدول العربية
إعداد: د .علي عبد القادر

23 - العولمة والبطالة: تحديات التنمية البشرية
إعداد: د .محمد عدنان وديع

24 - اقتصاديات التغير المناخي: الآثار والسياسات
إعداد: د .محمد نعمان نوفل

25 - المرأة والتنمية في الدول العربية: حالة المرأة الكويتية
إعداد: د .رياض بن جليلي

26 - البطالة ومستقبل أسواق العمل في الكويت
إعداد: د .بلقاسم العباس

27 - الديموقراطية والتنمية في الدول العربية
إعداد: د .علي عبدالقادر علي

28 - بيئة ممارسة أنشطة الأعمال ودور القطاع الخاص
إعداد: د .أحمد الكواز

29 - تأثير سياسات الترويج للاستثمار الأجنبي المباشر على قدرة الدول العربية في جذب هذه الاستثمارات لتحقيق أهدافها التنموية
إعداد: أ .منى بسيسو

30 - الاصلاح الضريبي في دولة الكويت
إعداد: د .عباس المجرن

31 - استهداف التضخم النقدي: ماذا يعني لدول مجلس التعاون؟
إعداد: د .وشاح رزاق

32 - الأزمة المالية الدولية وإنعكاساتها على دول الخليج
إعداد: د .وشاح رزاق
د .إبراهيم أونور
د .وليد عبد مولاه

33 - استخدام العوائد النفطية
إعداد: د .محمد إبراهيم السقا

34 - السوق الخليجية المشتركة
إعداد: د .أحمد الكواز

35 - الاقتصاد السياسي لعدم المساواة في الدول العربية
إعداد: د .علي عبدالقادر علي

36 - الضرائب، هبة الموارد الطبيعية وعرض العمل في الدول العربية ودول مجلس التعاون
إعداد: د. بلقاسم العباس
د. وشاح رزّاق

37 - إندماج إقتصادي إقليمي أم دولي: الحالة العربية
إعداد: د. أحمد الكواز

38 - التجارة البينية الخليجية
إعداد: د. وليد عبدمولاه

39 - تطوير الأسواق المالية التقييم والتقلب اعتبارات خاصة بالأسواق الناشئة
إعداد: أ. آلان بيفاني

40 - تقييم التجربة التنموية لدول مجلس التعاون الخليجي
إعداد: د. أحمد الكواز

41 - قياس كفاءة بنوك دول مجلس التعاون الخليجي
إعداد: د. إبراهيم أونور

علم الدين بانقا

42 - مُحددات الاستثمار الأجنبي المباشر الداخل إلى الدول العربية
إعداد: د .وليد عبد مولاه

43 - رأس المال البشري والنمو في الدول العربية
إعداد: د . بلقاسم العباس
د. وشاح رزاق

44 - لماذا لم تتحول أغلب البلدان النامية إلى بلدان متقدمة تنموياً؟
إعداد: د . أحمد الكواز

45 - حول حل معضلة بطالة المتعلمين في البلدان العربية
إعداد: د . حسين الطلافحه

46 - سجل التطورات المؤسسية في الدول العربية
إعداد: د . حسين الطلافحه

47 - المسؤولية الاجتماعية ومساهمة القطاع الخاص في التنمية
إعداد: د . وليد عبدمولاه

48 - البيئة الاستثمارية ومعوقات نمو المنشآت الصغيرة والمتوسطة: حالة دولة الكويت
إعداد: د . ايهاب مقابله

49 - التدريب أثناء الخدمة لشاغلي الوظيفة العامة: دراسة حالة لواقع التجربة الكويتية
إعداد: د . فهد الفضالة

50 - التكامل الاقتصادي: آليات تعزيز التعاون الاقتصادي العربي
إعداد: د . نواف أبو شمالة

51 - وكالات التصنيف الائتماني: عرض وتقييم
إعداد: د . أحمد الكواز

52 - دراسة تحليلية لأبعاد التحديات التي تواجه المشروعات الصغرى والصغيرة والمتوسطة ودور مؤسسات الدعم الفني
إعداد: د . إيهاب مقابله

53 - واقع المخاطر الإجتماعية في الجمهورية اليمنية
إعداد: د . محمد باطويح د. فيصل المناور

54 - تجارب تنموية رائدة - ماليزيا نموذجاً
إعداد: د. فيصل المناور د .عبدالحليم شاهين

المعهد العربي للتخطيط بالكويت

صندوق البريد 5834 صفاة 13059 دولة الكويت

: 24844061 (965) 24843130 : (965)24842935

: api@api.org.kw - www.arab-api.org

